TranScend™

User's Guide

Revision 2.122007

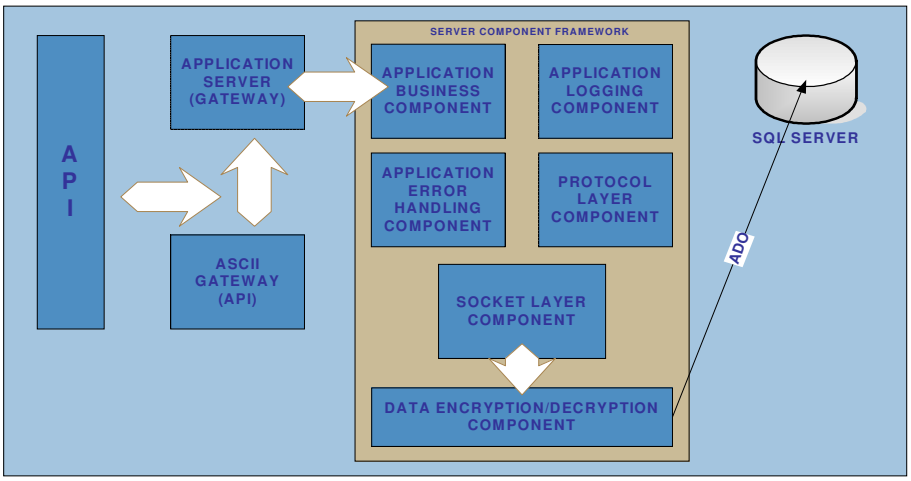
INTRIX Technology, Inc.
2260 Douglas Blvd., Suite 240
Roseville, CA 95661
Phone: (916) 577-1315
Fax: (916) 577-1316
Email: support@intrix.com

Table of Contents

Preface

Introduction

Congratulations on your purchase of TranScend™. TranScend™ is the newest, most powerful, and most flexible electronics payment system from INTRIX Technology, Inc. TranScend™ incorporates many features that are designed to provide constant and reliable payment processing services for your business. TranScend™ consists of a set of dedicated system services and a suite of client tools to enable quick deployment of the software system using any number of different deployment models as well as to provide easy to understand configuration and monitoring utilities so that you can tune the system to meet your own specific requirements.



System Requirements and Recommendations

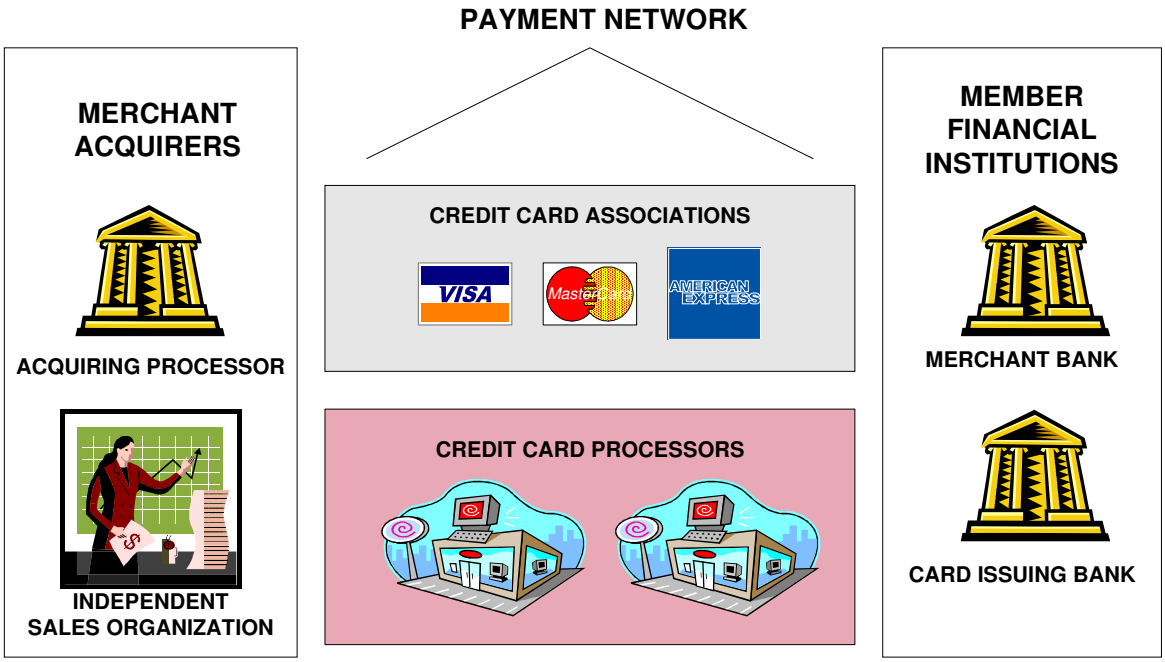
Hardware*	• Intel or AMD Processor: **> 2.0 GHz** (Or Greater) • 1 GB RAM (Or Greater) • 10 (Or Greater) GB of available Hard Disk space for log growth, database and virtual memory use • Available Serial Port for optional pin pads or receipt printer * SQL Servers Users should adhere to optimum SQL Server configurations which may be higher
Software*	• Windows 2003, XP, 2000 (Current Updates) • MS SQL, either Full or Express. * Anti-Virus applications should be cleared with INTRIX Support prior to use in conjunction with TranScend™

History of Payment Processing

Welcome to the world of payment processing. Whether you are an old hand at payment processing or new to the industry, this section will give you some relevant background as it relates to the payments industry.

The Architecture & Brief History of the Credit Card Industry

The credit card industry was born in the 1960s. Credit card banks (i.e., banks that exist primarily to issue credit cards) and non-bank issuers were an innovation of the '80s. The current architecture of the credit card industry evolved when the Bank of America renamed its "Bank Americard" as "Visa" and invented the payment network. A simplified model of this architecture is shown in Figure 1 below.



The payment network is the glue that binds the system together. The major firms in this arena are Visa, MasterCard, American Express, and Discover. (American Express and Discover are also issuers). The payment network maintains a merchant base which consists of merchants who accept the card and to whom the network forwards prompt payment when a cardholder makes a purchase.

The network charges the merchant a fee usually a percentage of the sale for this service. This fee is the primary source of revenue for the network and the "merchant acquirers" who manage the merchant base.

The network also maintains "member financial institutions" or banks that issue the network's credit card. The banks in turn "solicit" and build up a customer base of cardholders who will use their credit cards to make purchases from the merchant base and to obtain cash advances. The bank borrows funds from the money market and other sources and pays for the purchase at time t and then collects from the cardholder at time $t + n$ days, where n is typically between 30 and 120. The assets of the credit card issuer consist of the accumulated debt of the cardholders to the bank. The liability side consists of loans it took from the money market to pay the network for the purchase. It profits from a spread in the effective interest rate between the asset and liability sides and from seasoning its assets, that is, maintaining a high value of n. It may also generate revenue by charging various types of fees.

The spread that the bank actually earns is significantly reduced by charge-offs and back office expenses. The management of these expenses, particularly charge-offs, is the crucial factor in credit card bank management in a competitive environment. A spread of 7% can rapidly diminish to less than 2% with charge-offs in the 4% range. In a highly competitive arena, back office costs arise principally from origination and collection.

The Old Way

In the old days, credit card purchases were face-to-face transactions that required surrendering your card to the merchant, who placed it in something that looked like a small meat slicer covered it up with a sheaf of carbon papers, and rammed an imprinting bar across the whole mess. Everybody got a physical copy of the transaction-- the merchant, you, and the bank. The bank copies were accumulated throughout the day in a "batch", which was ultimately taken physically to the bank, or even mailed in an envelope. The merchant was responsible for keeping each piece of paper, which served as an accounting record; sales totals for the day had to be tallied up for each slip manually. The bank, in turn, had to manually tally up the slips too, so that the proper funds could be credited to the merchant's account. The bank then had receivables against the various card issuers for the total amounts of the transactions. The cardholder was then liable to the card issuer for payment of the deferred sale, and for most of us; this relationship of liability to the card issuer will endure for the rest of our lives.

The Electronic Terminal

Too much paper! Too much manual labor! Too many errors! With the computer age came a much better solution to credit card transaction processing. Instead of using the meat slicer, a merchant installed an electronic "terminal", which had a nifty magnetic stripe reader on the side, and some buttons to punch in the amount of the sale. The terminal would then dial up to a credit card processing center using a standard phone line, and receive authorization (or refusal) for the transaction. The terminal printed a receipt for the customer to sign, and both merchant and customer kept a paper copy of the transaction.

The terminal took much of the work load by transmitting the "batch" of transactions at the end of the day for settlement. Settlement consisted of the card processor depositing funds electronically to the merchant's bank. Still some paper involved, but much of the risk of doing "plastic" business was alleviated. Since authorizations were received electronically in real time, the merchant was assured of having a safe deposit able transaction. This method is still used predominantly today in point-of-sale situations such as restaurants, retail stores, gas stations—virtually any place where a customer is present, making a purchase with card-in-hand.

Mail Order/ Telephone Order (MOTO) Blossoms

The mail order industry blossomed with the advent of electronic credit card processing. Orders for products or services could be taken over the phone, and the terminal still had a role, only the customer obviously couldn't sign a receipt or present an actual card. This represented a larger risk to the credit card processors and merchant banks, because charges could be disputed—and favor usually smiled upon the cardholder, because there was no "proof" of the actual credit card being present for the transaction and no signature by the purchaser. For this reason, it has been historically difficult for catalog and direct mail businesses to establish a merchant account with a bank.

Goodbye, Terminal

It didn't take long for mail order establishments to discover that having each phone operator use a terminal to punch in a transaction (the magnetic stripe reader was obviously useless) was not very efficient. They were

also probably re-entering that same information into an order processing application of some kind on a desktop PC or mainframe terminal. What made more sense was to have the operator type the credit card information into the computer application, and somewhere in a back room, the transactions were all gathered into one point where they were transmitted to the processing company for approval—using a computer to do the job rather than a terminal. Simply write some software that makes the computer talk the same "language" that the terminal did.

Internet Commerce

Today, selling products and services over the Internet is commonplace. It's really no different than a mail order establishment, except that the customers enter their own order and payment information at their leisure. The web server application presents the buyer with an array of choices. The buyer selects the desired products or services, and types in a credit card number.

Now- In Simple Terms

The easiest way to understand the payments industry is to determine whether or not the card is present when the transaction is completed. Typically we view the amount of risk associated with a “card present” transaction to much less than one that is “non-card present”. Over the past few years growth has occurred in each of these segments and with the advent of smart cards, wireless networks, self-serve kiosks, security standards, micro-payments, etc. it’s likely that the payment industry will continue to grow significantly in the next several years.

Essentials of TranScend™

TranScend™ was developed with the maximum focus placed on the three S's of payment processing: speed, security, and simplicity

Speed, Security & Simplicity

The overall goal was to create a payment processing application able to support organizations regardless of their size, technical expertise, complicated configurations or existing reliance on legacy application.

Speed

Most application vendor's measure speed in terms of the total number of transactions processed over a given period time. TranScend™ can produce very admirable numbers using this formula. When configured properly and connected to a certified processor using an "always on" high speed connection, the merchant can experience multiple transactions per second.

The TranScend™ system utilizes several techniques to boost the data throughput of the system. Key among these approaches is the inclusion of asynchronous processing wherever possible within the system. Because of these processing optimizations, TranScend™ can process transactions at very high rates. In our "least powerful configuration" testing has shown transaction processing speeds as fast as 150 milliseconds per transaction.

Security

TranScend™ has used a *"Best of Breed"* approach as it relates to the implementation of security features. In most cases, decisions were made that surpass the best practice guidelines established in the Cardholder Information Security Program (CISP). Security methodologies are quickly becoming compromised by the ability to purchase database tools that allow informed users to decrypt database information. Think of it as a safe full of cash and safecrackers have learned how to open the safe. TranScend™ encrypts the data prior to entering the data into the database, so if it was compromised all that could be seen is a vast number of incoherent characters. Imagine a safe full of treasure maps written in a foreign language that would be nearly impossible to translate. Following are some of the specific approaches adopted in the implementation of TranScend™ that address the need of secure data handling:

Data Security

Data Security is becoming ever more important in all areas of commerce. Data Security is being demanded by the card associations, various governmental agencies, business' desire to mitigate undue risks, and by consumers as well. This being the case, TranScend™ was designed from the ground up with a strict approach to data security.

Session Level Security

All data communications between software components of TranScend™ data is secure. Prior to transmission of any data between programs, the two programs negotiate a unique session data encryption key. This data encryption key is unique between each two programs, and is valid only for the duration of that specific session.

Because each data exchange can happen in a unique session, each data transfer can have a different encryption key. This non-constant-key-schedule serves to provide the up-most level of data protection on the network. The data exchange protocol uses a 128-bit encryption using the blowfish encryption algorithm (selected for its speed) with further data security provided by several additional layers of data-packet CRC-validation in order to prevent "man in the middle" attacks.

Data Storage Security

All data that is stored in the TranScend™ database is encrypted prior to being stored in the database management system.

The implementation of this data encryption scheme is the AES encryption algorithm. AES was selected for the encryption algorithm as it is the recommended algorithm for data encryption by the NIST. The algorithm is further strengthened by the use of a rotating key schedule so that each value stored utilizes a unique 256-bit key for each data encryption operation. Here again, because a fixed key schedule is avoided in this scheme the security of the data is further enhanced.

User Security

The TranScend™ system utilizes several techniques in regards to user level access and control in an effort to provide further protection to the data stored in the TranScend™ database. First, with regards to user login-IDs and passwords, both of these values are passed through an exhaustive multi-round MD-5 oscillator which creates a one way hashing algorithm that prevents theft of user names/passwords as a means of compromising system security. Next, the rights and permissions for each user can be strictly controlled through assigning each user roles and permissions appropriate to their staff position within your organization. This approach will further safeguard payment data through preventing casual browses of data by any person that does not have express permission to do so.

Allowed IP Addresses List

To prevent unknown systems from attempting to connect to and/or attack the system, the system administrators can elect to provide a specific list of addresses that are allowed to connect to the TranScend™ system. For systems configured to use this feature, any system that attempts to connect to the system that is not on the allowed-address list will not be allowed to connect to the system.

Strict Message Validation with fail-fast session tear-down on message validation failures

All messages received by any process component of the TranScend™ system will be validated using several data checks. If any of these data checks fails, the process detecting the error will immediately and silently tear down the communications session. This approach of "silent death" of the connection is the approach recommended to thwart denial of service attacks as well as other common attempted system exploits. The approach also is designed to catch any data errors that may occur during message transmission and will prevent sending garbage out if garbage comes in.

Fault Tolerance

To address our customers' very valid expectations along with the stark realities of flaws in large software systems, TranScend™ is designed to be a fault tolerant and self healing system. In fact, several of the techniques adopted in the TranScend™ design were only previously available on much larger computing (the so-called mini-computer and mainframe platforms) systems. The fault tolerant aspect of the TranScend™ system is designed to provide our customers with 99.999% uptime. This translates into a much lower cost of ownership for customers of TranScend™.

Following are a list the fault tolerant approaches utilized in the implementation of TranScend™ along with what they provide to the customer.

Fail Fast Strategy

Some programs will still attempt to run even after they have encountered a "fatal condition" internally. The architects of TranScend™ system view this as a bad approach to the implementation of mission critical system design, because one should not trust a wounded program any more than they should trust a wounded animal. So, the approach adopted in all TranScend™ process is to "fail fast"—which means that they will quickly exit on any abnormal processing condition and will not continue to "limp along" in a wounded state on the chance that process in this state is just as likely to do as much harm as good in continuing in an abnormal processing condition.

Watch Dog Process

Recognizing that processes can fail fast (exit quickly on purpose due to some abnormal condition) or simply crash due to an undiscovered corner case (AKA a very well hidden program flaw), the TranScend™ architecture employs a process watch dog as a key component of the design. The TranScend™ "control server" is charged with making certain that all server processes in the TranScend™ server are alive and kicking. If any process is found to be down, the control server will restart it automatically without requiring any user intervention.

Self Healing Communications Channels

The TranScend™ system is coded with the expectation that the network is unreliable. With this in mind, all data communication channels are checked and validated as part of each message transmission. If the channel is found to be down, the session will be re-created as part of the data transmission. This approach ensures reliable data transmission between processing nodes which serves to increase the overall robustness and reliability of the TranScend™ system.

Data Journaling and Delta Records

The architecture of TranScend™ accounts for the fact that sometimes (for reasons only known by the database management system vendors) a database file can "go corrupt". This reality presents a huge risk to any company of catastrophic data loss. In response to this risk, TranScend™ utilizes several approaches designed to safeguard your company's data. One of these approaches is to employ a "delta record file" for all updates and changes to the TranScend™ database. The delta record file, along with TranScend™'s automated database backups can be used to quickly re-create a database image by providing a "replay capability" of your transaction data. In addition, the TranScend™ system utilizes a system of "journal files" to prevent loss of data prior to it being successfully stored in the database management system. In the event that any unit of work is not properly stored in the database management system, it can be manually captured from the delta record file or automatically captured from the TranScend™ journal files.

Automated Data Base Consistency Checks, and Archival Processes

TranScend™ includes an entire set of data management and database health-checks as part of its core processing system. These processes are designed to monitor and protect the data once it has been stored in the database management system. In addition, these processes help to maintain a healthy database by executing processes to detect and correct any non-fatal flaws detected in the database itself.

Data Mirrors

An optional TranScend™ module can provide complete database redundancy to the system. With the optional data mirror product, your TranScend™ system can be equipped with a complete "hot stand-by data base." Should any catastrophic event bring down the primary database in the TranScend™ system, you can quickly switch to the standby server and thereby keep your business up and running while the primary database problems are repaired. The TranScend™ system will also assist you with "re-synching" the primary database once it has been repaired.

Stateless Servers

All the processes in the TranScend™ System are stateless servers.

The **TranScend™** *System behaves in a strict command and reply architecture where each unit of work is treated as an ACID (Atomic, Consistent, Isolated, and Durable) transactional event. This approach allows for quick system recovery should any component in the system fail and have to be restarted, as there is no need to restore any previous program state in order for the system to return to a completely functional state. This strategy also minimizes the possibility of data loss caused by a process fault as there is no data held in memory in the servers that could be lost due to a process fault. Finally, this all or nothing approach is designed to maximize the consistency of transactions records.*

Distributed Computing Fault Tolerance

The processing model of the TranScend™ system can allow (note this feature is a purchase option) for a fully distributed deployment of the TranScend™ process components. The fault tolerance capabilities of the

TranScend™ control server include the ability to keep a fully distributed system up and running in a seamless manner such that the distributed system can be made to behave as a single "virtual server." This technology is unique in the industry, so that TranScend™ users that elect to utilize this feature are using the most advanced software system available for processing their electronic payment transactions. If you think this deployment model best suits your needs, please contact TranScend™ and discuss your requirements so that we can provide your organization with the most appropriately sized deployment.

Software That Grows With Your Requirements

Many other vendors offer several different products to address different business' data throughput or transaction type needs. This approach can create a difficult to understand mix of products which makes it hard to determine exactly which "version" of a product you will need.

Over time, the worst case scenario for your business if using one of these products is that your success will cause you to out-grow the product being used and you are then forced to "purchase up" to a completely different offering from that company.

A worse potential still is that these products may not even be compatible with each other (even though they may come from the same vendor) or are not easily upgraded which puts your company's transactions-data at risk of loss and/or premature retirement.

To counter this possibility, TranScend™ offers a unique and more beneficial product plan; wherein the TranScend™ system can grow in capability as your business grows. TranScend™ offers a single code base for a feature rich product. The features of the product are controlled by the product key.

Therefore, if initially your business demands for your payment processing system are minimal, you can purchase TranScend™ with some of the more advanced product features disabled and/or "throttled down". Then as your business grows, you simply need to purchase a more feature rich product key that enables the features that best fit your new expanded requirements. With this approach, simply installing a new valid license key will enable you to "upgrade" your installation without having to change a single bit of installed code.

This more thoughtful approach to product packaging allows your business a more robust and reliable and simplified upgrade path and also prevents the risk of any data loss due to any upgrades. In addition, it allows you to select which features are important to your business and provides you with much more flexibility in what you purchase as part of your payment processing system.

In the next section, we'll look at some related features of the system design that allow the system to scale well. These features will allow your TranScend™ system to grow in capability and processing power (data throughput) as your business grows. It is important to keep in mind that many of these features are controlled by the product license key, and depending on how your system requirements evolve, you may need to purchase new, more feature enabled, product keys.

Redundancy and Scalability

In a previous section, the fault tolerance techniques used in TranScend™ were explained to provide you with information on how the system design approaches a maximum uptime philosophy. Those features are included in the TranScend™ product so that the product's reliability becomes a near-zero concern for the user.

Another major concern for business owners is the long-term-utility of any product that becomes a "core component" of the business. The last thing that any business owner wants is to disrupt their business in order to replace a key component that can no longer keep up with the new demands of the business. Recognizing

the concern, the TranScend™ system is designed to scale in processing power in many ways. Therefore, scalability became a key consideration in the architecture and implementation of the system. There are many approaches to product scalability utilized in TranScend™, which are listed below:

Multiple Outbound Communications Channels

The connection to the card processor is by far the slowest part of the system processing performed by TranScend™. In fact, our internal testing shows that if a typical transaction is processed in 200 milliseconds, better than half that time is spent exchanging data with the card processing company. To account for this factor, all processes that connect to the card processors employ a connection pooling strategy where multiple connections to the processors are made (if the card processor allows this). Each of these communication channels can execute "in parallel" for separate client requests, which serves to boost the throughput of the system overall.

Optional Configurations

The TranScend™ system allows for multiple instances of some processes. For example, if your installation has a large number of simultaneous users, then you can purchase additional processing power in the form of allowing multiple system gateway servers to run simultaneously. With this configuration, you could set up your system so that users are load balanced across multiple gateway servers. This configuration will allow the system to provide improved response times to user requests by distributing the load related to the number of connected users across multiple system connection points. Another example of an optional configuration that can boost system throughput is to allow for multiple authorization and batch servers to run simultaneously. Since we already recognize that the connection to the processor is the primary contributor to transaction processing times, load sharing simultaneous requests to the card processor across multiple authorization servers will increase the throughput of processing transactions in larger installations.

Fully Distributed Computing Model is Supported

The TranScend™ system is designed to allow a fully distributed installation. If your system has exceptional data volumes and/or throughput requirements, you may also opt to purchase a system license that will allow you to distribute the TranScend™ processes across multiple servers to gain additional processing power from the system. This configuration is made possible by the "self discovery mechanisms" built into the TranScend™ systems that allow the components of the TranScend™ system to "automatically discover" other processes that form the core of the TranScend™ data processing system. In addition, this solution leverages the very unique distributed-computing-system start-up and control system built into the TranScend™ control server.

Processor Portability

Over time you may find that competition within the payment processor marketplace will allow your business to gain a significant per-transaction cost reduction by switching to another payment processor. To allow you to benefit from these opportunities, TranScend™ can be easily reconfigured to send your transactions to another payment processor (contact TranScend™ sales for the current list of processors supported by TranScend™). Since this a simple reconfiguration of the TranScend™ system, and does not involve any other changes to your system, there is virtually no risk in executing a "mid-stream change" of this nature.

Split Dial

In some cases, businesses that accept multiple payment types may seek the "best prices" when selecting processors to perform interchange services for different payment types. In the most extreme of these cases,

the business may have a different card processor for each payment type accepted. To allow your business to benefit from these possibilities, TranScend™ is designed with several levels of "split dial" capability, which the term we use when your business has a desire to employ "multiple targets" for different payment types.

TCP/IP Settings

TranScend™ requires use of the TCP/IP network protocol for communications. Prior to installation of TranScend™, TCP/IP must be installed. Your network configuration may currently have TCP/IP settings statically assigned (manually configured), or dynamically assigned (automatically configured) through DHCP (Dynamic Host Configuration Protocol). If your network has TCP/IP settings statically assigned, have your TCP/IP information available when configuring TranScend™. Sites that use DHCP will need to assign or reserve a static TCP/IP address for their TranScend™ server processes.

NOTE*:* Contact your Network/IS Administrator to verify/satisfy the requirements mentioned here.

TranScend™ is designed to work in a network environment, but it does not require a NIC (Network Interface Card) to operate properly.

Emulation Mode

After installing TranScend™, you will notice that it is running in **Emulation Mode**. This mode is a testing environment; all transactions are simulated and the actual communication to the Credit Card Processor does not occur. This allows for extensive testing of TranScend™ features and also development of a custom interface with your products. TranScend™ will constantly remind you that you are in emulation mode when the server is started. Within the transaction message response you will see the indicator "(FAKE)". To activate TranScend™ for real-time credit card processing, call your Sales or Support representative at INTRIX Technology, Inc. (800) 546-8749, during or after purchase.

Transaction Processing

Card present transaction process, non-card present transaction process, and transaction process summary.

The Card Present Transaction Process

Steps involved in a card present transaction:

1. Merchant calculates the amount of purchase and asks buyer for payment.
2. Buyer presents merchant with a credit card.
3. Merchant runs credit card through the point of sale unit. The amount of the sale is either hand-entered or transmitted by the cash register.
4. Merchant transmits the credit card data and sales amount with a request for authorization of the sale to their acquiring bank.
   Point of sale units are usually set to request authorization at the time of sale, and then actually capture the sales draft at a later time.
5. The acquiring bank that processes the transaction, routes the authorization request to the card-issuing bank. The credit card number identifies type of card, issuing bank, and the cardholder's account.
6. If the cardholder has enough credit in their account to cover the sale, the issuing bank authorizes the transaction and generates an authorization code. This code is sent back to the acquiring bank.
   The issuing bank puts a hold on the cardholder's account for the amount of the sale. Note that the cardholder's account has not been actually charged yet.
7. The acquiring bank processing the transaction, and then sends the approval or denial code to the merchant's point of sale unit. Each point of sale device has a separate terminal ID for credit card processors to be able to route data back to that particular unit.
8. A sale draft, or slip, is printed out by the point of sale unit or cash register. The merchant asks the buyer to sign the sale draft, which obligates them to reimburse the card-issuing bank for the amount of the sale.
9. At a later time, probably that night when the store is closing up, the merchant reviews all the authorizations stored in the point of sale unit against the signed sales drafts. When all the credit card authorizations have been verified to match the actual sales drafts, the merchant will capture, or transmit, the data on each authorized credit card transaction to the acquiring bank for deposit. This is in lieu of depositing the actual signed paper drafts with the bank.
10. The acquiring bank performs what is called an interchange for each sales draft, with the appropriate card-issuing bank. The card-issuing bank transfers the amount of the sales draft, minus an interchange fee to the acquiring bank.
11. The acquiring bank then deposits the amount of the all the sales drafts submitted by the merchant, less a discount fee, into the merchant's bank account.

The overview presented above is far from complete. It does not cover the role of the financial networks, nor of the bankcard associations. Also, it is geared towards Visa and MasterCard transactions. There is no card-issuing bank with American Express and Discover. These shortcomings aside, the sequence of events

outlined above provides a good overview of the credit card payment process. It will also give you something to look back at as this document discusses methods for performing online credit card transactions.

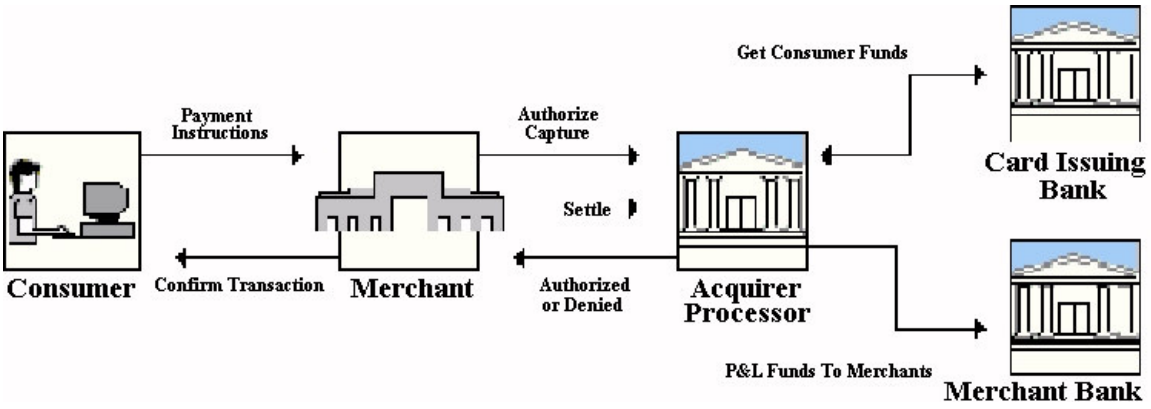
The Non-Card Present Transaction Process

Non-card present transactions require two steps: authorization, and after product has been shipped, settlement (also called funds capture). The merchant is legally bound to wait until the product ships before settlement can take place. The credit card process consists of five different parties:

- ✓ **Card Holder**, or customer, who makes a purchase using a credit card
- ✓ **Issuing Bank** extends credit and provides the Card Holder with a credit card
- ✓ **Merchant**
- ✓ **Merchant Bank** issues a merchant account to the Merchant
- ✓ **Credit Card Processor** authorizes and manages the transaction through the financial network

In some cases, the Merchant Bank and Credit Card Processor are combined and referred to as the **Acquiring Bank**. The Merchant Bank, however, can assign another institution (Credit Card Processor) to act on its behalf for handling transactions through the financial networks.

Credit card data can be manually entered into an electronic cash register, software program, or swiped via a magnetic stripe reader. The magnetic stripe on a credit card normally has several "tracks" of data that are parsed to get the card number, cardholder's name and the expiration date.



Credit Card Transaction Process Summary

Following is a basic scenario for credit card transaction:

- Consumer decides to purchase service or products from Merchant. Submits information to merchant.
- The merchant sends the consumer information to the Credit Card Processor for authorization.
- The Credit Card Processor either authorizes a certain amount of money (issues an authorization code) or declines the transaction.
- If the transaction is authorized, a "capture" takes the information from the successful authorization and charges the authorized amount of money to the consumer's credit card.

- If the consumer cancels the order before it is captured, a “void” is generated; if the consumer returns goods after the transaction has been captured, a “credit” is generated.
- Then Settlement occurs. Captures and credits usually accumulate into a “batch” and are settled as a group. When a batch is submitted, the merchant’s payment-enabled server connects with the Credit Card Processor to finalize the transactions and transfer monies to the Merchant bank account.

Step 1: Authorization

Although non-card present transactions are not usually settled at the time of order taking, it is a good idea for the merchant to get an immediate authorization prior to shipping the product. The merchant electronically submits a request to the *Credit Card Processor* to find out if the customer has enough credit. The *Credit Card Processor* in turn contacts the *Issuing Bank* and passes on the card number, expiration date and purchase amount. The *Credit Card Processor* gets back an *Approval Code* and informs the merchant. This whole process only takes a few seconds.

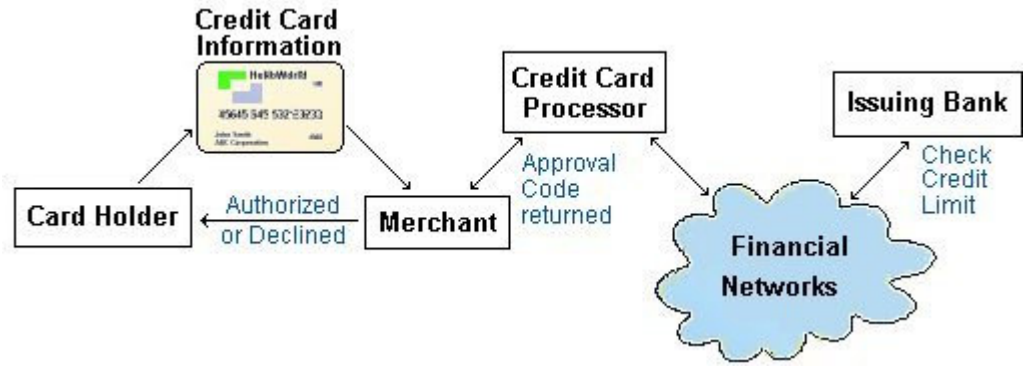


Figure1: Authorization

Although *Authorization* alone does not cause an exchange of funds, it does reduce the cardholder’s *Open to Buy* amount, the credit available from the *Issuing Bank*. This works to the advantage of the current merchant, since later purchases with other merchants cannot use the allocated authorization amount.

If the Authorization of a transaction never goes to settlement, the amount held against the cardholder’s account will normally expire in 7-10 days.

NOTE: For authorizations that expire, when an item is on back order, a new Authorization can be submitted.

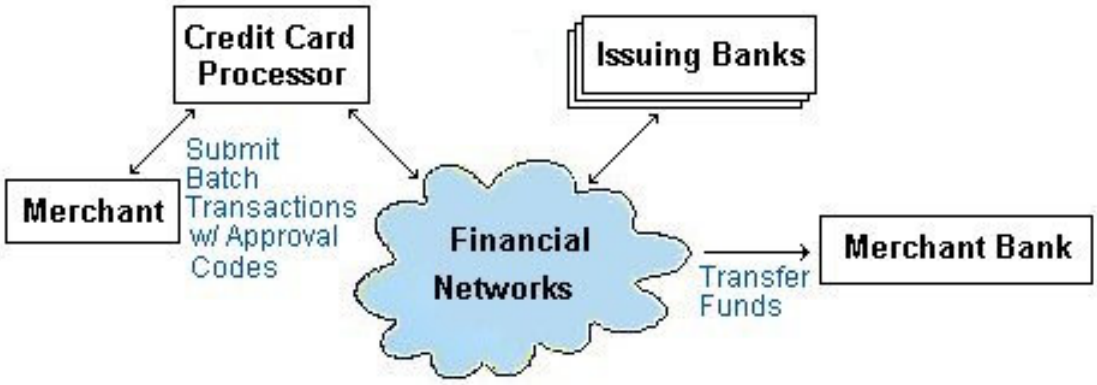
A *Reversal* (or void) transaction can be made against an Authorization, but not all Issuing Banks support reversals. Whether or not the issuing bank honors the Reversal, TranScend™ will remove the Authorization transaction from the Settlement batch. A settled transaction cannot be reversed, but see "Credit" transactions, below.

NOTE: TranScend™ transmits data on Reversals for Visa transactions since Visa honors Reversals. All other credit cards do not honor Reversals; these are only handled internally by TranScend™ as mentioned previously.

Step 2: Settlement

Non-card present merchants normally collect all of the authorization records into a batch and settle them at one particular time of the day. High volume sales merchants, however, may need to run several batches throughout the day. *Capture* is the process of converting an existing authorization into a settlement

transaction record within the outgoing batch. See the figure below for an illustration of the settlement process.



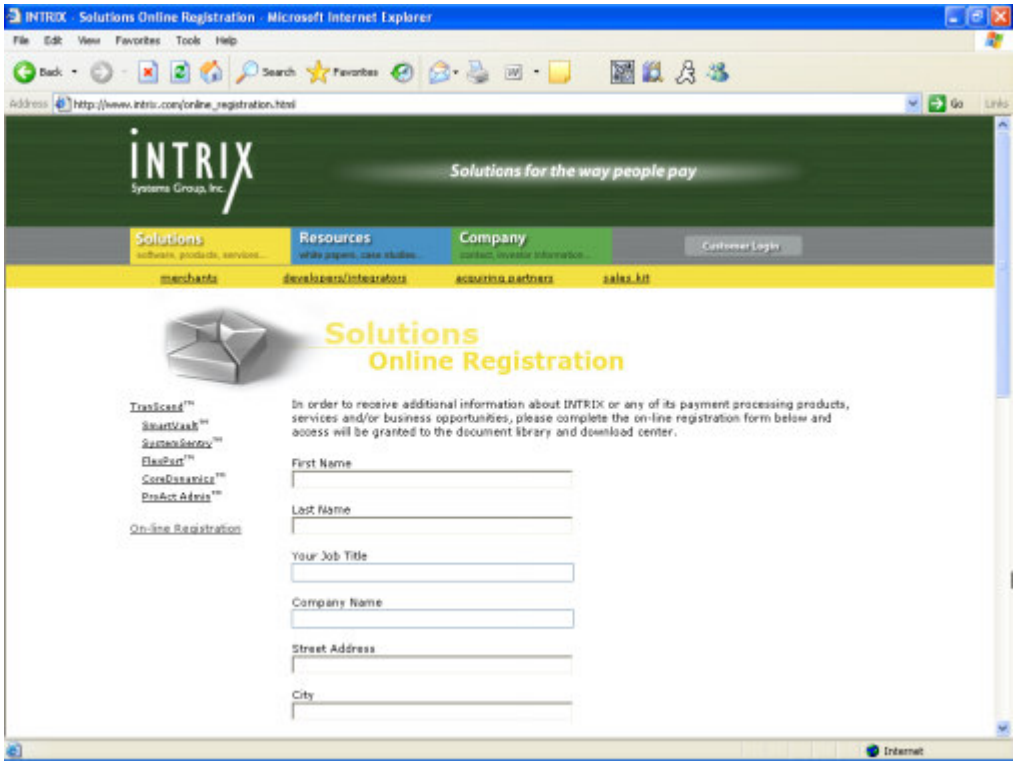
Step 2: Settlement

If a customer returns an item after authorization and settlement, the Merchant can issue a *Credit* transaction to the Credit Card Processor that will return the funds from the Merchant Bank back to the Card Holder's account. Prior to settlement it is possible to adjust the dollar amount down in the settlement, which is useful for handling partial shipments

TranScend™ Download and Registration

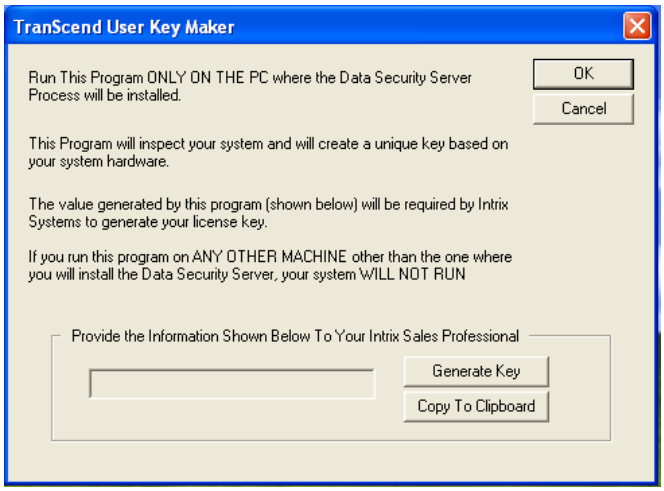
Register to Download TranScend™

- Open Web Browser (e.g. Internet Explorer)
- In the address field type: http://www.intrix.com/online_registration.html



Register to Download TranScend™ through Internet Explorer

Accurately complete the registration form and click on submit. An email will be sent shortly after registration to the email address provided. The email will contain a link with download and installation information. Once downloaded and installed, you now have all the necessary components to install and operate the TranScend™ software in "Emulation Mode".

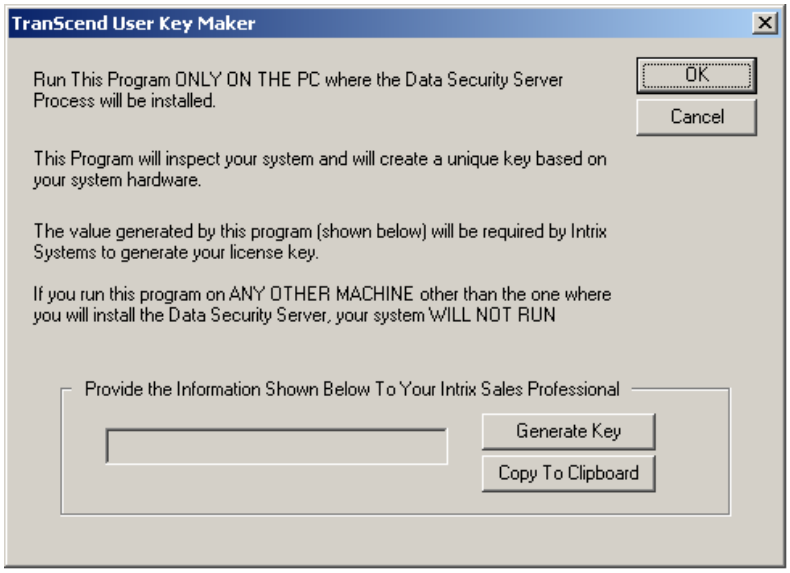


TranScend™ Registration

A significant time and focus has been placed on the ability to move TranScend™ from an Emulation test mode configuration into either a full production system or an end to end processor test configuration. INTRIX Support will provide a Registration Key that is locked to a specific piece of hardware. For non-expiring keys, full payment must be received prior to go live date. As always, we offer a Try before You Buy options. In order to register, perform the following steps:

Step 1

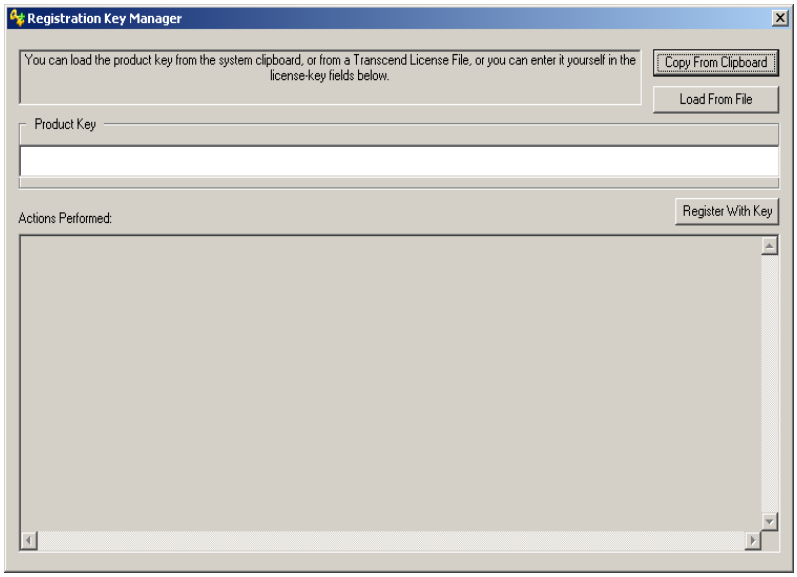
- Click on “Start” Button
- Click on “All Programs” menu item
- Click on “ITI_TranScend” menu item
- Click on “TPA Key Generator” menu item



Step 2

- Click on the “Generate Key” button
- Click the “Copy To Clipboard” button to paste this information into an email that can be sent to support@intrix.com and upon payment, a Registration key will be sent back to you.

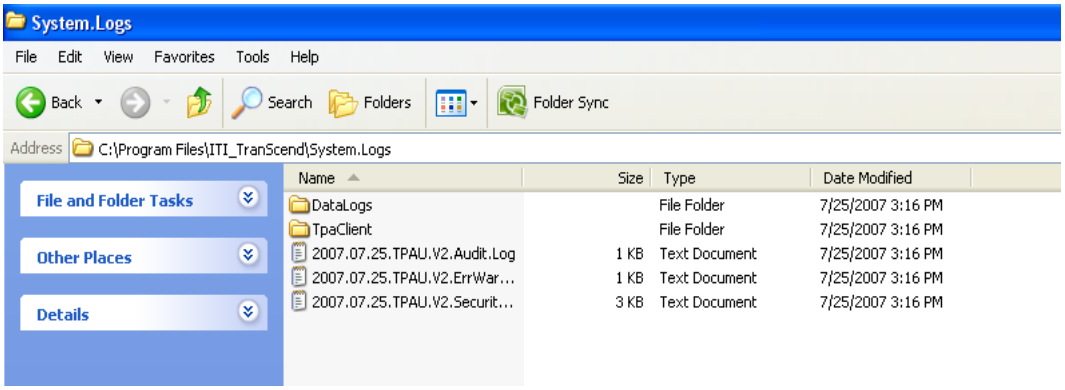
Step 3



- Click on “Start” Button
- Click on “All Programs” menu item
- Click on “ITI_TranScend” menu item
- Click on “TPA License Key Manager” menu item
- Click on either “Copy From Clipboard or Load From File” Depending upon how the information was received from INTRIX Support
- Click on “Register With Key”. Note that this will log you on to the TranScend™ system, so be certain that the TranScend™ Servers are running. Once the logon is completed, the new product key will be loaded into the TranScend™ system.
- Restart your servers (stop and start them) using the TpaTray program.
- After restarting your servers, you will now be able to configure TranScend™ with the appropriate processor specific setup information.

TranScend™ Logs

After TranScend™ has been downloaded, installed and registered; the installation process will have created a directory structure similar to the diagram below. (Assumes default install path was chosen during installation)



The Log Server provides a system wide logging mechanism for TranScend™. Since there are a number of processes included in the system, that each will generate messages to be stored in the system log, there is a need for a single process to collect and manage this information. This function is provided by the Log Server.

The design of the Log Server is focused primarily on speed so that logging does not have an adverse affect on the overall throughput of the system. Therefore TranScend™ *utilizes a system of asynchronous logging from all the processes. This approach has a side-effect that messages may "arrive at the log server out of order."*

Even so, this is not necessarily a problem as the log server can be optionally deployed to utilize a file-based, SQL-database as one of the storage formats for log messages. So, if time-ordered-views are important, then the log-server's database can be viewed for those types of log analysis exercises. Further, as this is an SQL database, this data can be filtered with specific. SQL queries to provide highly clarified views of the log data.

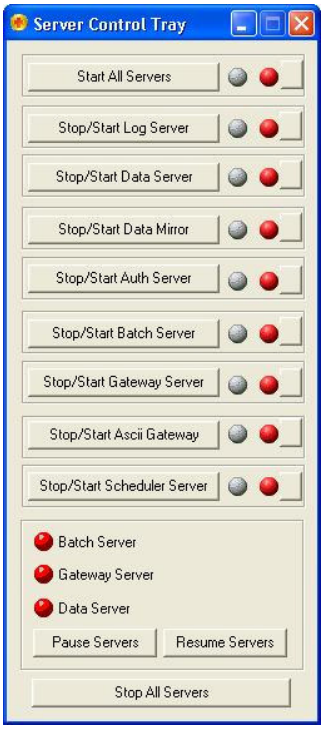
The Log Server provides log data storage in flat-text files for easy "quick views" of log output from the system. The log server creates 3 text files for each day's operations: the "security log file", the "audit log file" and the "errors and warnings log file". The "security log" is a file that contains information about each login attempt to the system. It also logs which IP addresses are allowed to connect to your system. The "audit log" contains only those messages which are "audit events" encountered during processing. "Audit events" are those messages which have to do with either money or card-processor communications. "Money messages" encompass any log message that has to do with the transfer and/or handling of electronic payment processing. The "errors and warnings log" contains only those logged messages that are either warnings or errors reported by the system. Normally, the "error and warning log" should contain no messages whatsoever. If any messages are found in this file, then this indicates a potential system issue that should be investigated.

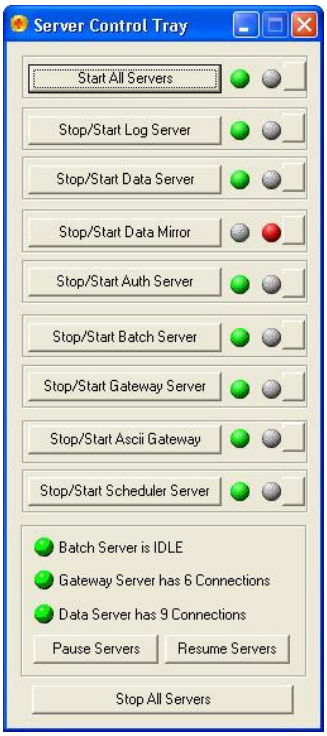
The log server manages these files automatically, thereby making the system more “self-managing” which reduces the burden on the user of the system with regards to the management of these files and the disk space they consume. The first way these files are managed, is that the Log Server employs “midnight processing” which means that each day “yesterday’s log files” are automatically compressed and added to a zip file. Therefore, the “zipped log” contains a single day’s log data files for longer-term storage. Secondly, the “zipped logs” that are older than 60 days (this is the default value, the actual number of days is a configurable parameter) are automatically erased from the system.

If you have elected to utilize the optional Alerts Services of TranScend™, then the log server will also provide an additional service; which is to generate an email alert whenever a message is written to the “errors and warnings” log. This purchase option benefits the user in that the system will let the user know when an error or warning has occurred. Without this feature, the user will have to examine the “error and warning log” to determine if any system errors had happened. The optional Alerts Services allows the system to take a more pro-active approach in communicate to the owner/administrator that a non-optimal system state was detected.

The Log Server is also one of the “programmable components” of the TranScend™ Application Server. Purchasers of the TranScend™ Application Server Development Kit will be shown that the behavior of the Log Server can be enhanced to perform functions specific to your company requirements as part of observing and processing the system’s log-data stream. When the “extended log” functionality is made part of a larger system integration that includes your “external systems” inserting “custom messages” into the TranScend™ log-stream, then your system can offer a certain degree of customized “closed loop” processing with regards to customized programming of the TranScend™ system.

Starting and Stopping The TranScend™ Servers





Before any processing can occur with TranScend™, the system must be started. TranScend™ ships with a utility program called the "Control Tray" which serves a centralized control point for starting, pausing, and stopping the TranScend™ servers.

The image on the left shows this program as it appears when all the TranScend™ servers are stopped. To start the system from this status, one only has to click on the "Start All Servers" button on the top of the program.

When this action is performed, the Control Server will start and then it will start all the other servers in the system. The Control Server also monitors the running state of all other system servers, and if any of them are down, the Control Server will restart them in order to keep the system ready to process your transactions.

To stop the TranScend™ servers, simply click on the "Stop All Servers" button on the bottom of the Control Tray Program. If the Control Tray Program is minimized, it will still appear in the System Tray as a pair of "four leaf clovers" so that the system's status can still be viewed at a glance.

The buttons to the far-right of the "indicator lights" can be used to open a "server view" window. The server-view window allows the user to watch messages that are produced by the various servers as the system is running. Server-Views can be closed by clicking the close box in the upper-right corner of their caption bar.

When the servers are running, the Control Tray should appear like the image on the left. Here you can see that all the "green indicator lights" are showing that the system servers are all up and running.

Finally, the Control Tray can be used to Pause and Resume the system as it is running. If the TranScend™ servers are paused, what this means that is "no new transaction processing" can be accepted by the system. However, work any pre-existing transactions that are currently being performed when the system is put into a pause status will be allowed to complete.

The purpose of pausing the system is to allow for any orderly shutdown of the TranScend™ system for periodic maintenance or system updates in order to minimize the possibility that any "transactions in flight" will be lost when the system needs to be stopped.

The best way to stop the system is put pause it, then stop all connected clients, then when the Batch Server and the Gateway Server report they are idle, it is safe to stop the system completely.

Once the system is Paused, the Gateway may not go to a complete idle state until all clients are stopped. Also, the ASCII Gateway is a specialized form of system client that can be stopped in an orderly manner as follows:

1) Click the "Start All Servers" button to stop the Control Server. Once it is stopped, the "Red Indicator" in the top row will "light up.
2) Click the "Stop/Start Ascii Gateway" button to stop the ASCII Gateway. Shortly after this servers stops the Gateway will become idle unless there are more clients running somewhere in the network.

TranScend™ Client

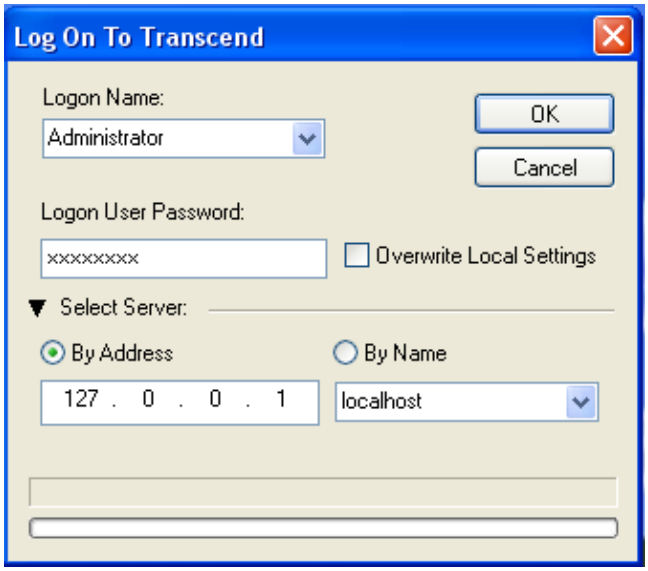
Overview

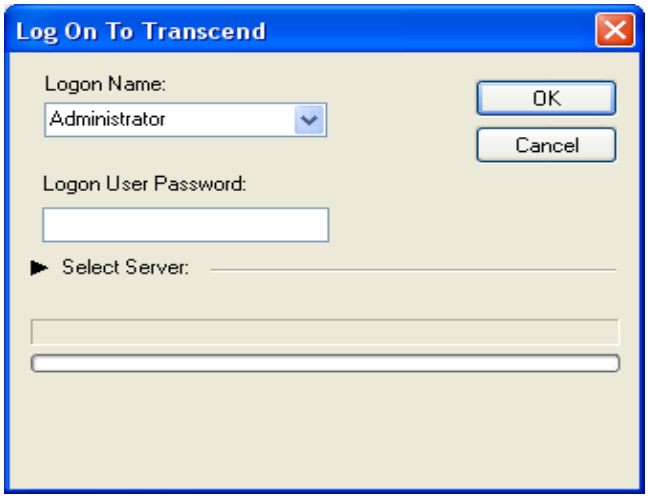
TranScend™ Client runs in unison with the TranScend™ Servers; thus, the TranScend™ Servers must be running in order to use TranScend™ Client to process credit card transactions. You can process a number of different types of payment transactions (Processor Dependant) which may include Credit Cards, Gift Cards, EBT and Checks. Credit Card transactions in most cases include purchases, credits, authorizations, batch releases(Settlement or Capture), and reversals. Gift Card transactions in most cases include activations, redemptions, and balance inquiries. Gift cards in most cases include activation issuance, redemption, balance inquiries, and deactivations. EBT transactions include sale, prior sale, returns and balance inquiries. Checks can include Point of Purchase (POP) and Accounts Receivable Conversion (ARC) transaction sets. With just one click of a button, TranScend™ Client sends credit card information to the TranScend™ Server for processing and displays the results within seconds.

		
TranScend™ Client >	TranScend™ Server >	Credit Card Processor

The TranScend™ Client also has some information features such as a Console for showing TranScend™ Server Status and Up Times Statistics, as well as measurements of transaction throughput times. A extensive reporting tool for printing receipts, detailed transaction data and batch information for reconciling. TranScend™ Client plays a number of useful roles within an eneterprise. You can use it as a point of sale mechanism or to browse, create, modify, and purge transactions. It is used to configure many of the TranScend™ including merchant and user setup, communications and fraud mechanisms such as AVS and CVV2 parameters.

Logging In





To Open TranScend™ Client, Navigate the main system menu to locate and start the program as follows:

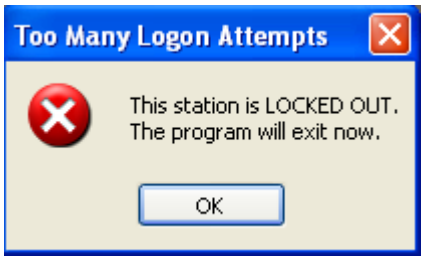
Click on START→All Programs→INTRIX Technology→TpaClient menu command to show the logon screen that appears on the left.

The login screen will retain the "Last known good" parameters with exception of the password which, for security purposes, must be entered each and every time a user logs in. The login can be attempted either by the specific IP address of the TranScend™ servers or by DNS server name. A successful login will retain the desired settings so user can simply enter the password and Click OK without needing to know the specifics for Server selection.

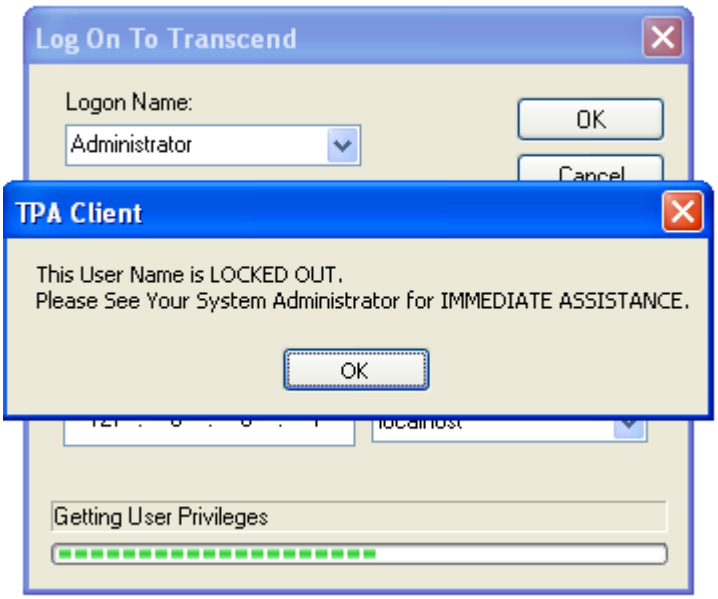
The Server Selection option can be hidden by clicking the ▼icon resulting in a login screen that looks like this to minimize confusion for less capable users:

Logon Failures

If the credentials you supplied are not correct, then you will see the message box (shown at the far left) appear on the screen. After this, you will be presented with the main logon screen again so that you can try again. If there are too many logon attempts that fail, then the workstation will become locked out and you will be shown a screen like the one on the right.



Note: *The station lockout feature is required by VISA and PABP and the feature can not be bypassed or removed. Once a workstation has been locked out, then the system administrator will be required to use the LIN utility described in Appendix G of this document.*



The next time that a logon is attempted from any locked out workstation, the user attempting the logon will be shown the screen to the left. This will occur even if the user credentials are good because the user's name has already been added to the lockout list.

It is also worth noting that "User Lockouts" will be automatically expired by the system in one half an hour. So, if a user locks themselves out, and the administrator can not be located to correct the situation with use of the LIN utility, then that user account will become automatically re-enabled by the system after one half hour passes.

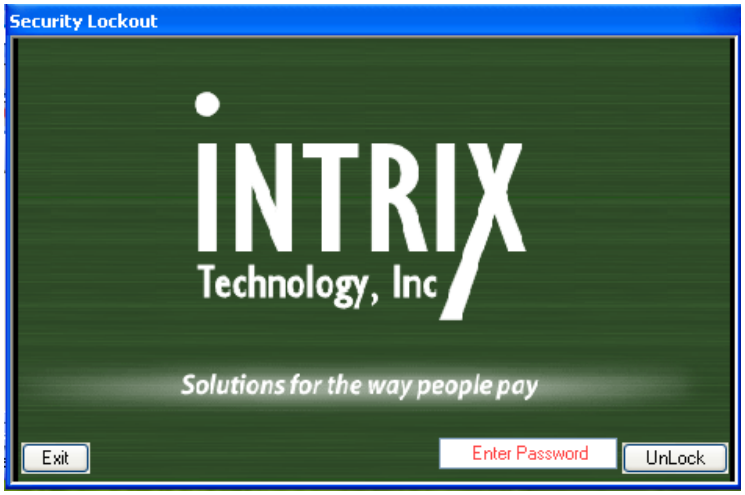
There is another type of lockout that is more permanent. This is called a station-lockout. In this kind of lockout, the workstation itself was judged to be insecure through repeated failed logon attempts.

In order to prevent data break-ins from an insecure terminal, the workstation's address is added to the lockout list. A station lock out *never* expires, and *must be* removed by a system administrator with the LIN program. This security feature is designed to prevent attacks from unknown or not properly secured clients. For more information on clearking stations lock, please see Appendix G for more information on the use of this utility.

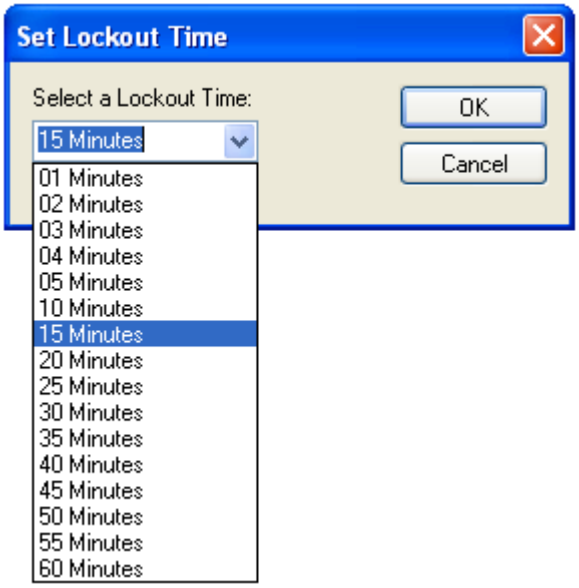
Screen Lock Login

The TranScend™ Client features an additional safety measure known as a Screen Lock Timeout. When a client program is logged in and user has been idle for a given period of time, the client will lock itself. The lock out time is user definable from 1-60 minutes with a default of 15 minutes. The user can also immediately lock their client screen by clicking on the menu command: File→Lock Screen.

The client lock-out screen is shown below. Note that if there are too many failed logon attempts from the screen lock, the workstation will be viewed as not secure and the workstation address will be added to the locked out list. For assistance with clearing locked out stations and users, see Appendix G for usage of the LIN utility.



A user can change the Screen Lock timeout at any time. In order to accomplish this, the user would click the menu command: File→Set Screen Lock Time. The dialog shown below will then be shown to the user which offers a wide range of possible timeout values to select from.



Commands and Help Menu

Commands Menu

Change Password

A logged on user can change their password at any time. In order to accomplish this, the user would invoke the command found in Commands→Change Password in order to display the dialog shown immediately below. In order to change the password the user must enter the current password (to prevent unauthorized password changes) and the new password twice (so that the new value can be confirmed). Here are some helpful things to know when creating a new password:

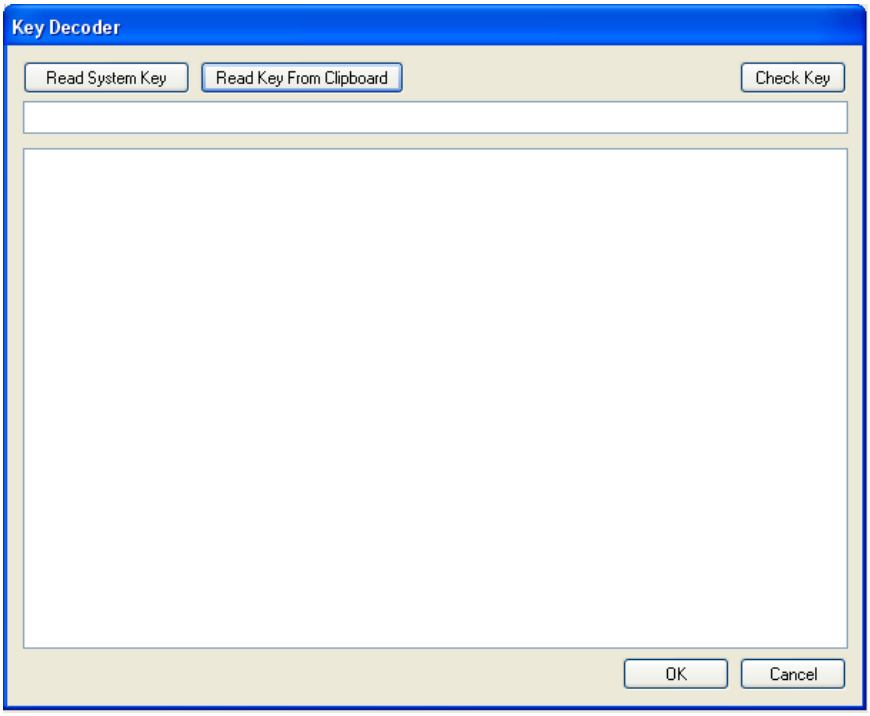
- Change password first
- Make password unique by combining letters and numbers
- Password must be at 8 characters long
- Passwords can only last 90 days

It is important to note that when a user changes their password, it will take effect on their next logon. If a user changes their password, then remains logged into the system, and their client enters a screen locked state, then the user must use their current password to unlock the client program.

Help Menu

Decode Product License

Invoking this command will display a dialog like the one shown below. Here the user can test system license keys in order to discover what the users of that key are licensed to do with their installation of TranScend™. Keys can either be pasted from the clipboard or the system's currently installed key can be read from the TranScend™ system servers and decoded in the window shown below:



Configuration

The Configuration Options are your tools to configure your system for fraud filters, configure merchants and to set up your users. You will find that the Administration Menu is valuable to enable you to make the best use of what TranScend™ Products can do for you while maintaining security. Within the Configuration Tab, you will notice the following items: Configure System, Configure Merchants, and Configure Users. In this part of the next section you will become familiar with the Configuration Options for initial set up and ongoing service.

TranScend™ Centralized Configuration

or

Diagrams of TranScend™ Centralized and Distributed Configurations

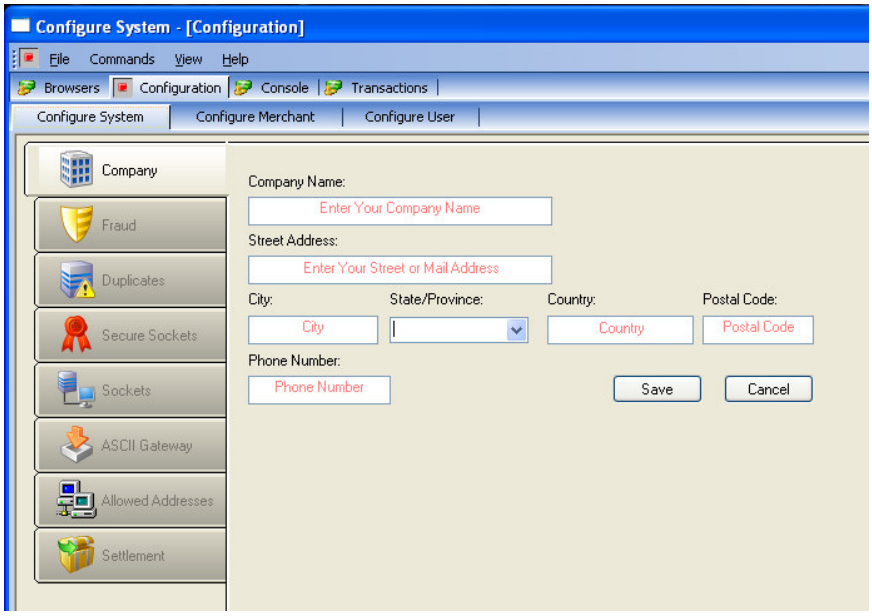
Configure System

The Configure System Tab contains options for configuring Company information, Fraud Filters, Processor communication options which include: Secure Sockets (Internet SSL communications to the processor) and Sockets (Leased Line connections to the processor). The Application Programming Interface option known as the ASCII Gateway has some user configurable options. Allowable IP Addresses configuration is an integral part of the security features of TranScend™. And finally, Settlement allows for batch times to be set for various merchant groups.

Creating the Company

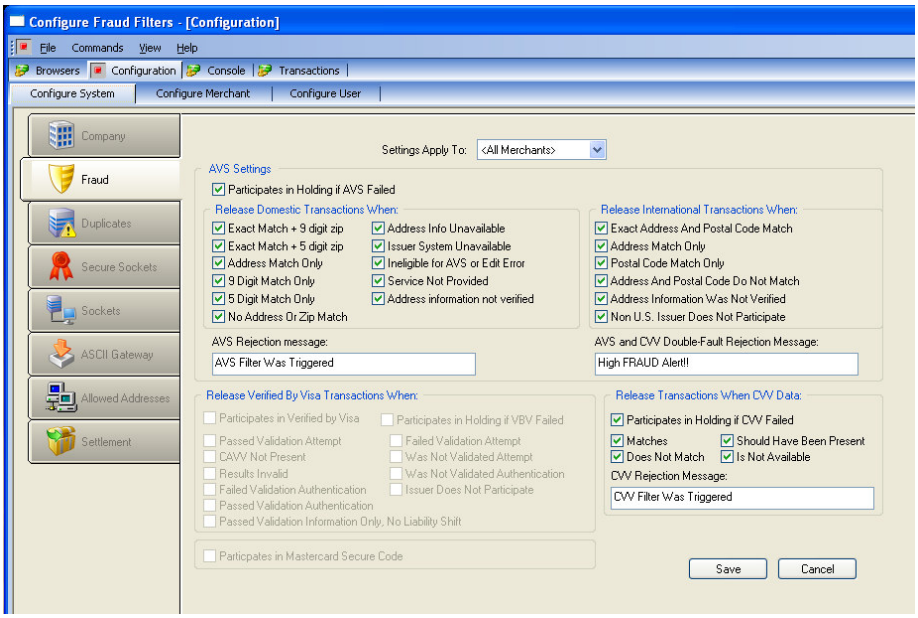
- Login to the TranScend™ client utility
- Click on the "Configuration" tab
- Click on "Configure System" tab
- Click on "Company" tab
- Click "Save" when done

Enter all pertinent company information and click the "Save" button. This information can be drawn upon and used later when configuring merchant accounts as well. Clicking "Cancel" will back out any unsaved changes and restore previously saved information.



Configure Fraud Filters

In addition to the approved response provided by the Credit Card Processor, you may be provided with an AVS (Address Verification Service), a VBV (Verified by Visa) and/or a CVV (Card Verification Value) response for transactions containing the appropriate customer. Often times, these additional responses will have no bearing on whether the transaction is approved or not.



For example, a transaction can still be approved even if the address doesn't match. To assist merchants reduce fraudulent activity, TranScend™ provides an optional filtering mechanism which can take non-desired AVS, CVV or VBV responses and place the transaction in a "H=Authorized/on hold" status. When a transaction is placed in a "H=Authorized/on hold" status, TranScend™ does not ready the transaction for settlement.

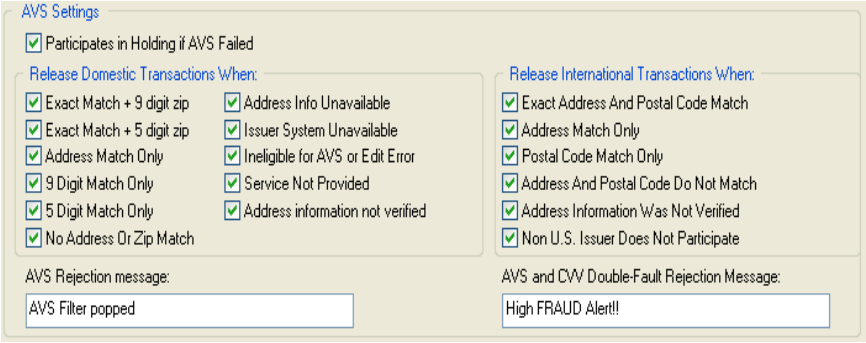
The merchant can manually release a transaction from a "H=Authorized/on hold" status after appropriate investigation through the API Mechanism or Client in order to allow the transaction settle. Please note, the default settings ensure that all "Match" type responses are released and therefore immediately eligible for settlement. Theses settings can either apply to an individual merchant or all merchants. These settings can quickly and easily be tailored for any businesses rules or policies.

AVS (Address Verification Service)

AVS is the process of verifying the address and/or zip code submitted with the transaction against the address and/or zip code listed on the cardholder's monthly statement. Direct Marketing and MOTO industries have always benefitted from this service, and retail is now finding ways to utilize this feature. If during a Retail transaction and the card cannot be read, the merchant may receive preferred rates by including the zip code with the transaction.

Setting the AVS Fraud Filters

- Click on responses to Release for Domestic AVS Responses and International Transactions
- Click on "AVS Message Text:" to enter a suitable message which will be returned as a part of the transaction response.
- Click "Save" to save the changes.



VBV (Verified By Visa)

VBV is the process of validating a card holder created password that is submitted with an online transaction. The cardholder must enroll into the program to establish the password for the card and the merchant must participate and have the necessary plugins on their website. These Optional measures applies to participating merchants in the Electronic Commerce industry. MasterCard has a similar feature known as **MasterCard SecureCode**.

Setting the VBV Filters

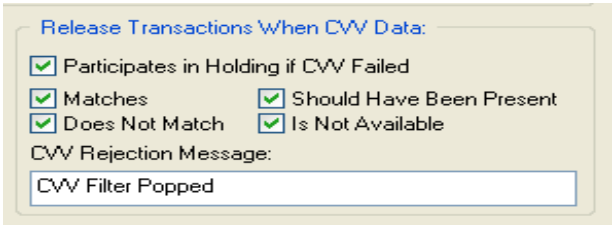
- Click the appropriate responses to "Release Verified By Visa Transactions When:"
- Click the "Participates in MasterCard Secure Code"
- Click "Save" to save the changes.

CVV (Card Verification Value)/ CID (Cardholder ID)

CVV values are the last 3 digits located on the back of Visa, MasterCard and Discover cards in the signature bar. CID values are the 4 digit (Unembossed or flat) number on the front of American Express cards always located above the account number. These additional measures help ensure physical card presence thereby reducing fraudulent usage during a non-face-to-face transaction.

Setting the CVV/CID Filter

- Click the appropriate responses to "Release Transactions When CVV Data:"
- Click "Save" to save the changes.

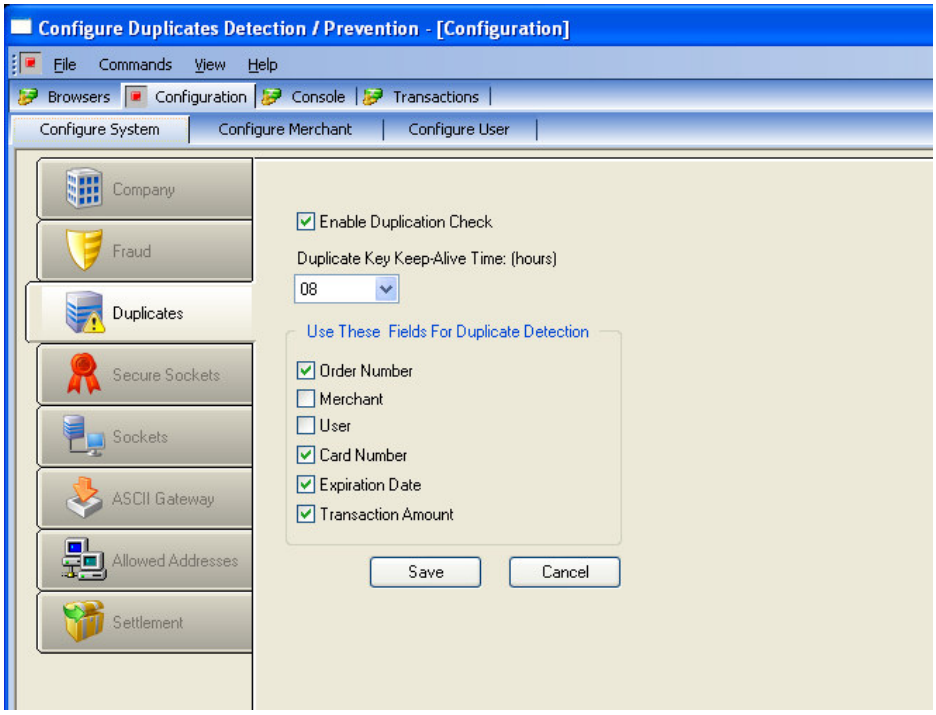


Configure Duplicate Checking

TranScend™ contains a duplicate transaction mechanism to help prevent unwanted duplicate transactions. When configuring the duplicate transaction parameters, the user must take into account current business practices to ensure that the settings are stringent enough to catch errors but lenient enough to allow for any necessary subsequent transaction processing. For example, some merchants allow for their customers to call back within a certain amount of time and add on to previously placed orders. If this process involves a prior authorized amount, a new transaction may need to be entered for the recently added goods or services. In this case the Duplicate Checking parameters might be set to trigger the duplicate if the dollar amount matches but not trigger if the dollar amounts differ. The Duplicate Checking works against the user defined time interval (Default is 8 hours). If more time is necessary to ensure non-duplicates, the number of hours should be adjusted accordingly.

Setting the Duplicate Transaction Parameters

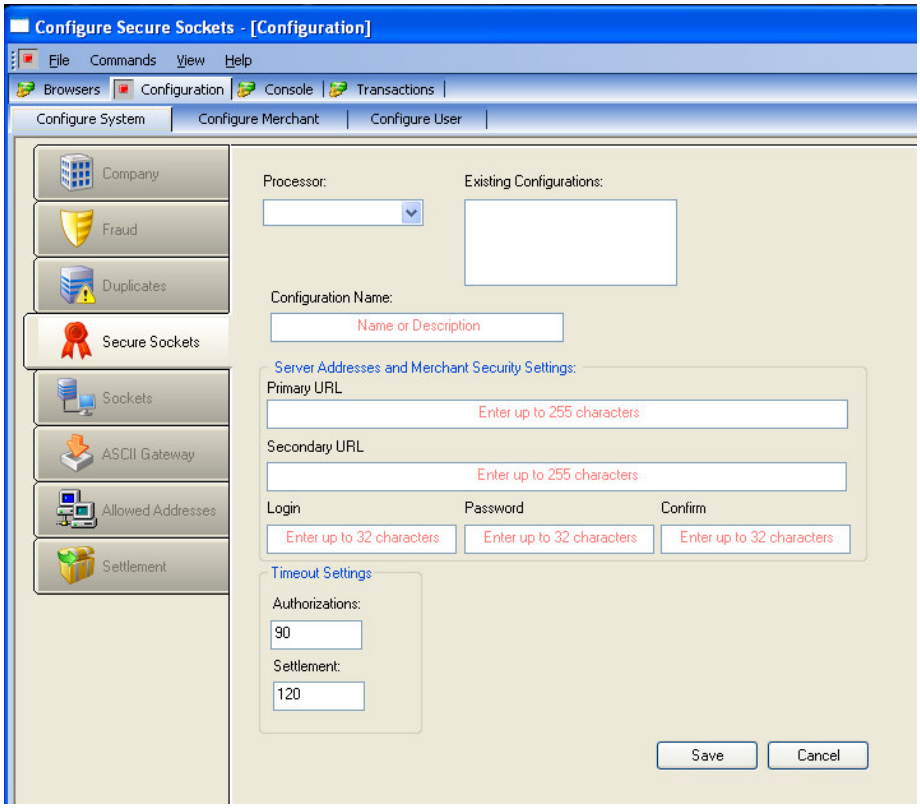
- Click “Enable Duplication Check”
- Click to adjust the Keep-Alive hours
- Click to adjust Fields to be included in duplicate checking
- Click “Save” to save the changes.



NOTE: The Authorization Server must be restarted for the changes to take effect

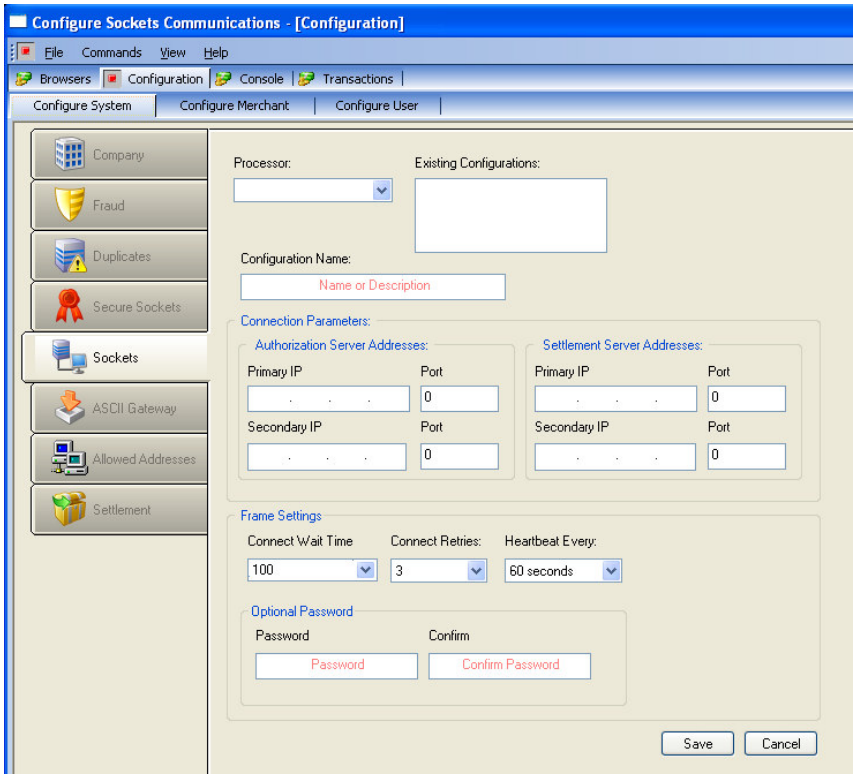
Configure Secure Sockets

The Secure Sockets configuration is intended for merchants who have already configured their merchant account with a processor for internet processing. TranScend™ utilizes industry standard SSL encryption to protect the data prior to sending the information to the merchant's card processor. This screen allows a merchant to set up the connection parameters so that TranScend™ can connect to the internet via the merchant's internal network. An "Always On" or Broadband connection is highly recommended and can produce transaction response times on the order of 2-5 seconds.



- Click Drop Down to select "Processor"
- Click Configuration Name field to name the SSL configuration appropriately (Example <Processor Name> SSL)
- Click to enter primary URL as specified by the processor
- Click to a secondary URL if specified by the processor
- Enter the appropriate URL login information as provided by the processor.
  NOTE: Not all processors require this information so verify with you processor.
- Timeout settings should be left at the default values unless otherwise instructed to change by the INTRIX Support Staff
- If your environment uses a Proxy Server for web access, consult your system administrator or network personnel for the appropriate information needed to complete the proxy settings.
  NOTE: Not all locations utilize a Proxy Server.
- Click "Save" to save the changes

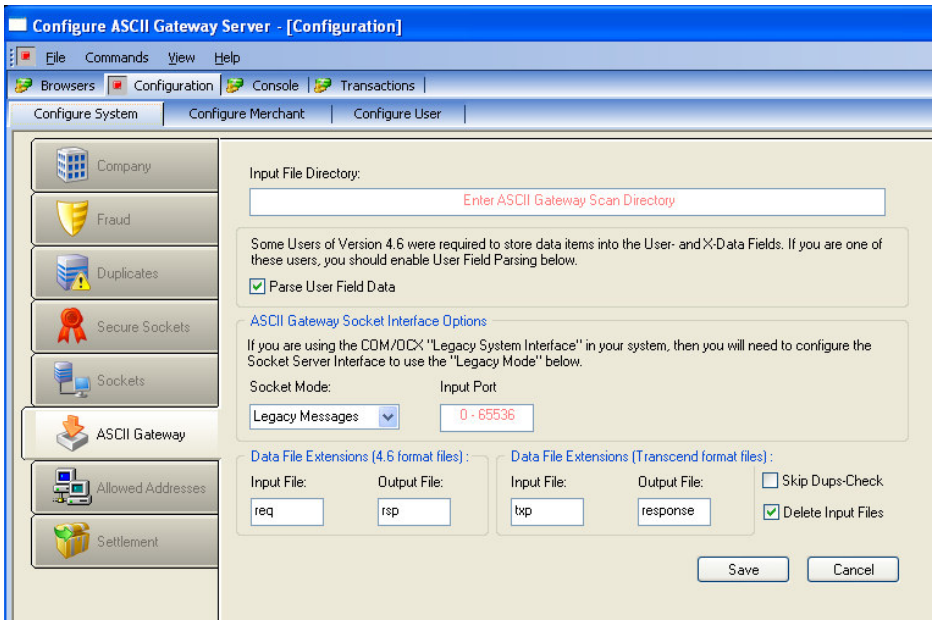
Configure Sockets (Frame Relay or Leased-Line Connections)



The Sockets configuration is intended for merchants who have already made arrangements with the processor to provision a dedicated Leased-Line to the processor. Advantages of the dedicated connection include 24/7 monitoring by the processor, truly seamless failover as many routers have either analog or ISDN modems connected, and a blazing fast transaction response time of 1-3 seconds. In most cases, the processors alert customers of Leased-Line communication related issues before the customers are even aware they are experiencing issues. The configuration can easily be completed once the processor has provided all of the necessary connection information. NOTE: the computer itself will require information to be added to the IP Route Table in order for the IP addresses entered into this screen to be reached. The Leased-Line installer will cover all of this during testing and the processors network support staff can assist with changes made to the Leased Line connection parameters.

- Click Drop Down to select “Processor”
- Click Configuration Name field to name the Socket configuration appropriately (Example <Processor Name> IP or Lease Line)
- Click to enter primary Authorization IP address and Port as specified by the processor
- Click to enter primary Settlement IP address and Port as specified by the processor
- Click to add a secondary Authorization IP address as provided by the processor
- Click to add a secondary Settlement IP address as provided by the processor
- Connect Wait Times, Connection Retries, and Heartbeat settings should be left at the default values unless otherwise instructed to change by the INTRIX Support Staff
- If your processor has required the use of a Password, please enter it here and confirm the entry. **NOTE**: Not all Leased Lines require a password login so consult the Leased Line installation representative.
- Click “Save” to save the changes

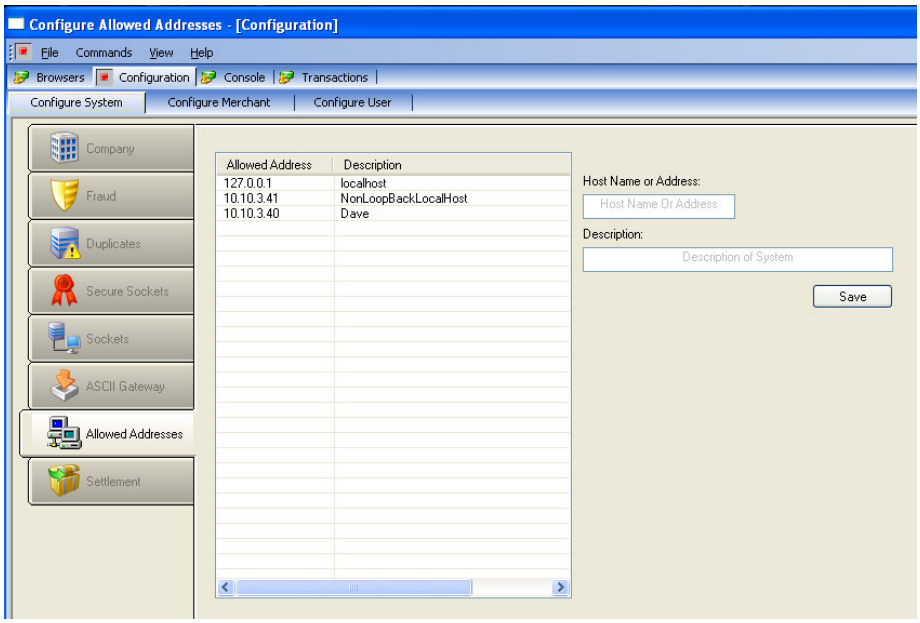
ASCII Gateway



This configuration screen allows the user to specify the appropriate input file or Drop directory (Default is: C:\Program Files\ITI_TranScend\ScanDir). SuperCharge 4.6 users who pass additional data elements in via the user data fields (User Defined Data, Combined Extract Data or Lodging) must select The Parse User Field Data when using the legacy API structure. This screen also allows the user to specify the connection port and the message format. SuperCharge 4.6 users wishing to retain their original message formats must select the Legacy Messages. Users wishing to take advantage of new features associated with the TranScend™ and have written to the Enhanced Message Format new to TranScend™, will want to select the Enhanced messages option. Data file extensions for either the legacy 4.6 or the TranScend™ format are user definable. The default for 4.6 has always been .req for requests and .rsp for response files. Two additional options are to have TranScend™ delete the clear text transaction request file upon file load completion (Recommended for PCI/CISP Best Practices. Users may also override TranScend™ Duplication Checking (See Section 3.5.3), while this is NOT recommended, there may be strong business cases that necessitate this feature being disabled.

- Click “Input File Directory” to change for appropriate file drop zone (Default is C:\Program Files\ITI_TranScend\ScanDir\)
- Click “Parse User Field Data” if you use User1-User4 data fields on SuperCharge 4.6 for processor specific data elements. Contact INTRIX Support if you have specific questions. The default will cause no harm.
- Click “ASCII Gateway Socket Interface Options” to specify Legacy Messages (SuperCharge 4.6 Format) or Enhanced Messages options (New TranScend™ Format) and then specify an Input Port (Default is 2000).
- Click “Data File Extensions either 4.6 format or TranScend™” to specify appropriate file extensions. Default SuperCharge 4.6 is .req for request and .rsp for response. TranScend™ defaults are .txp for requests and .response for response file.

Allowed Addresses



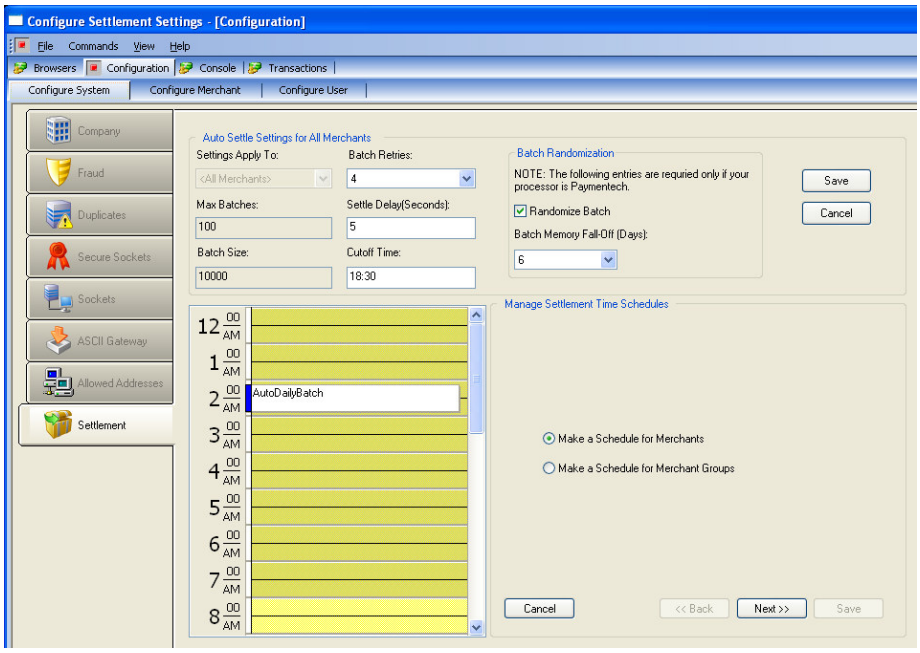
To prevent unknown systems/users from connecting to and/or attacking the system, system administrators can elect to provide a specific list of addresses that are allowed to connect to the TranScend™ system. For systems configured to use this feature, any unauthorized attempts to connect to the system (Attempts that are not granted access in the allowed-address list) will not be allowed to connect to the system. Logging will record each attempt in order for the threat to be dealt with.

- Click “Host Name or Address” to enter the allowed DNS name or IP Address.
- Provide a Description for each new entry.
- Press Save to add new address.
- Entries can be removed by highlighting the entry and performing a Right Mouse Click and selecting delete.

Settlement

The Settlement Configuration allows user to setup Auto-Settle parameters for TranScend™

- ❖ Click “Settle Delays” when your processor has indicated to do so. This is the minimum allowable interval specified by processors from when a transaction can be authorized and then settlement can be performed.
- ❖ Click “Cutoff Time” to specify the time which begins the new transaction period for the day. For example, if all business up to 3:00 PM is considered today’s business, this entry should be 15:00. If all transactions received prior to midnight are considered a day’s transactions, leave this entry at 23:59.
- ❖ Click “Batch Retries” only if instructed to do so by INTRIX Technology, Inc. personnel. Otherwise, this entry may result in multiple settlement scenarios and upset your customer base.
- ❖ Click “Auto Settle Time” to adjust the time TranScend™ will automatically begin the settlement phase of transaction processing. The optimal time for your business may have been specified by your processor and should be entered here in military time format.
- ❖ Under special circumstances for Paymentech Tampa customers, you may need to turn on batch randomization. This in effect randomizes your batch sizes to bypass Paymentech’s duplicate batch checking methodologies. EXTREME CAUTION should be used when selecting this option. Duplicate batches can result causing your customers to become very upset. If you are unsure what this option does, please contact INTRIX support (800) 546-8749.
- ❖ Click “Save” or “Cancel” to either commit the changes or to begin the configuration again.



NOTE: The Batch Server must be restarted for the changes to take effect

Merchant and Privilege Group Information

How do I obtain a Merchant ID and other Merchant Information?

Contact your merchant's bank to obtain valid information when you are ready to go "live" and process credit card transactions using TranScend™. What you do with the information depends on the device you will use to communicate with the bank.

Configure Merchants

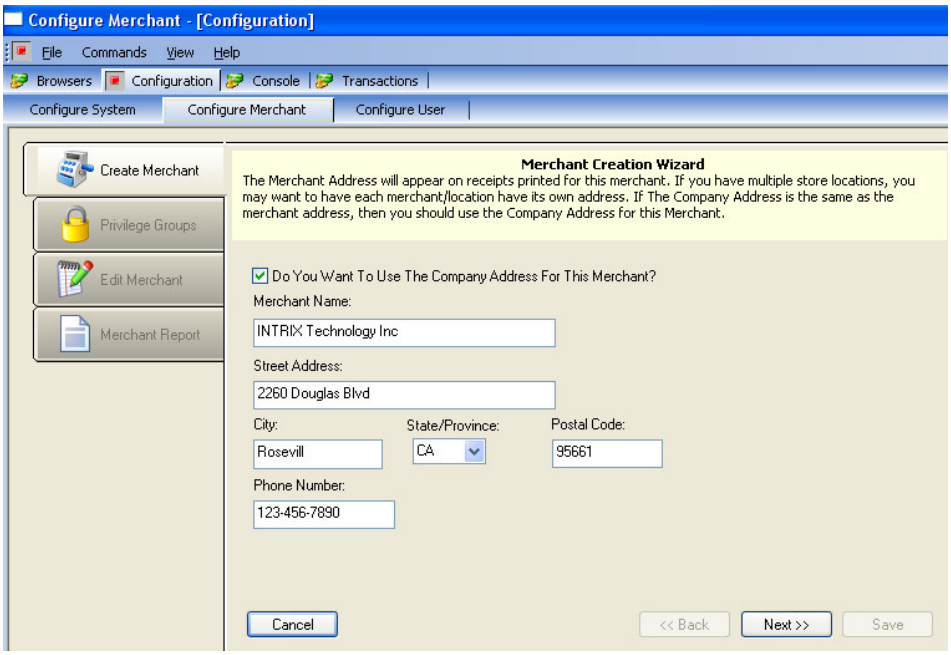
The Merchant Configuration Wizard will guide you through the merchant configuration procedure. The Wizard has been designed to only show you the configuration screens necessary for the payment processor you have chosen for you business. Also note that your processor communications (SSL, Sockets or Modem) should have already been configured prior to starting to configure your merchant's settings.

NOTE: Please be sure to have your Merchant Configuration Sheet in hand before proceeding with the creation of a new merchant.

Create Merchant

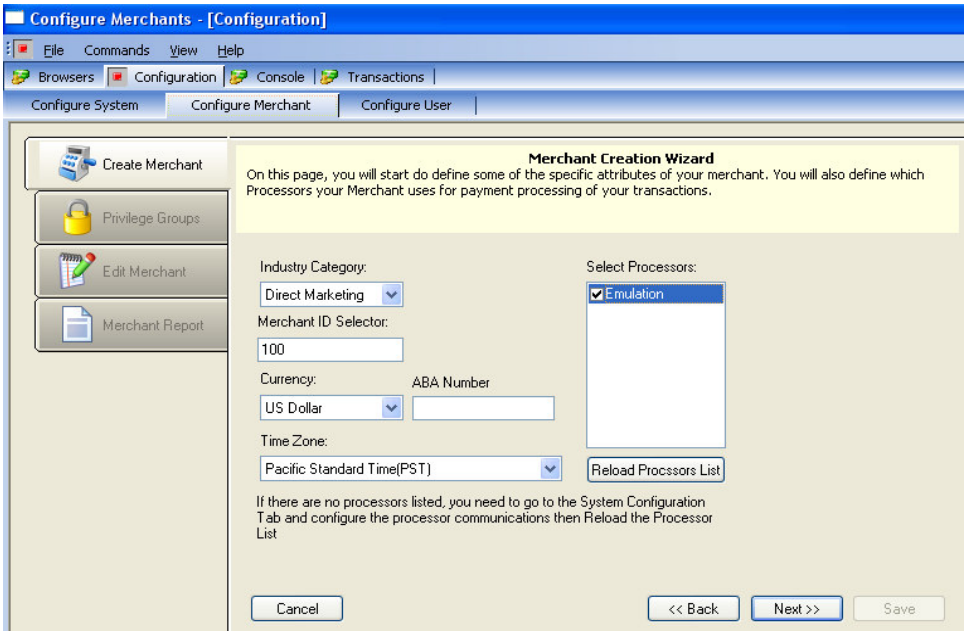
Step 1

- Login to the TranScend™ client utility
- Click on the "Configuration" tab
- Click on the "Configure Merchant" tab
- Click on the "Create Merchant" tab
- Enter your merchant name and business address
- Click "Next"



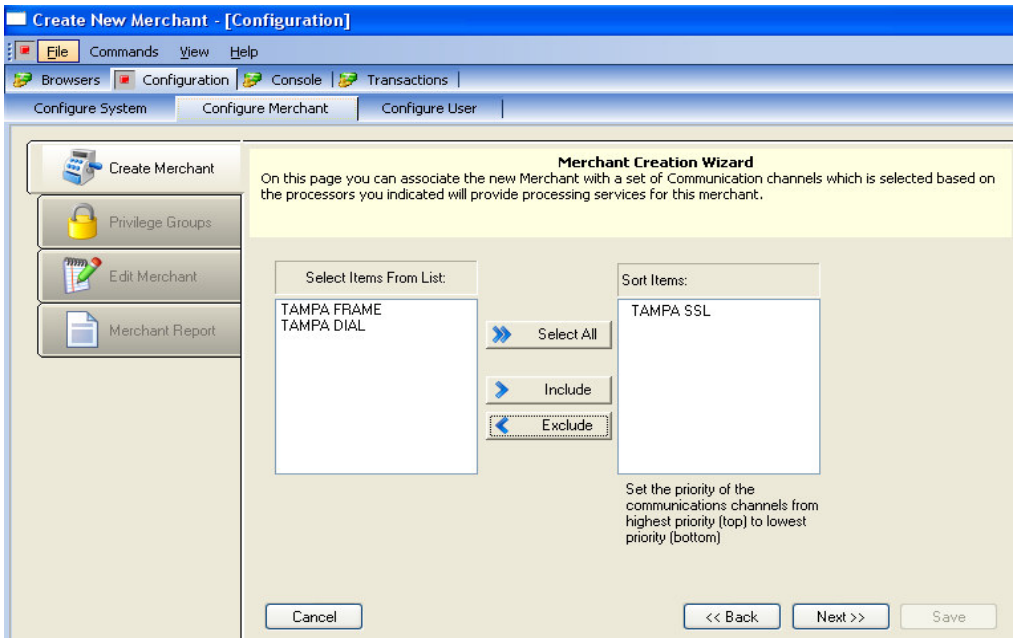
Step 2

- Enter your "Industry Category"
- Enter a unique "Merchant ID Selector"
- Enter "Currency" type
- Enter "ABA Number" (optional)
- Enter "Time Zone"
- Select Processor
- Click "Next"



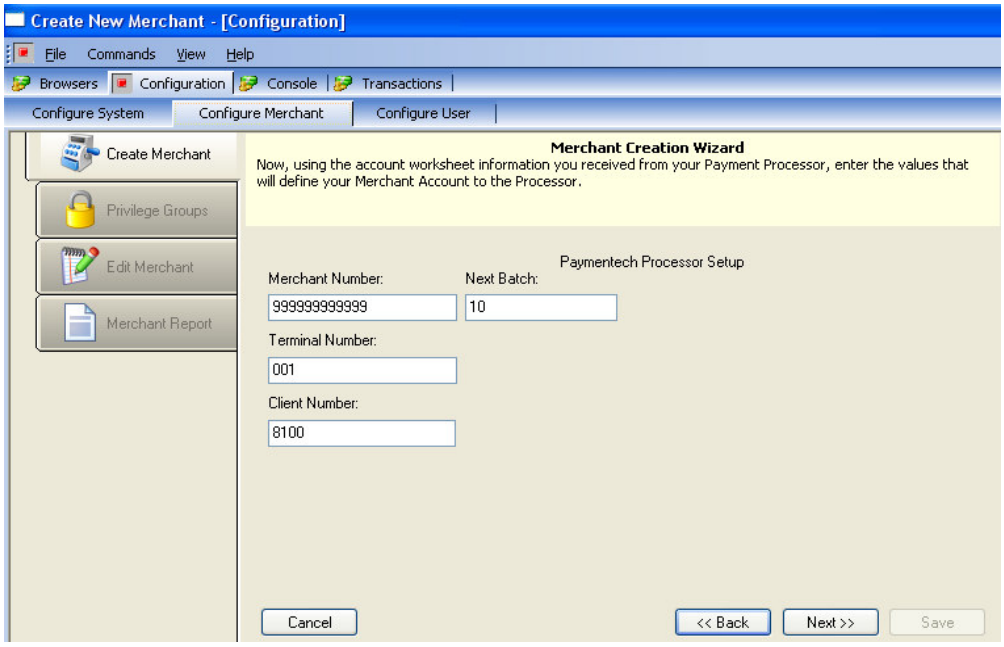
Step 3

- Select your "Communication Methods"
- HINT: As you select the methods, be sure to put them in "rank order"
- Click "Next"



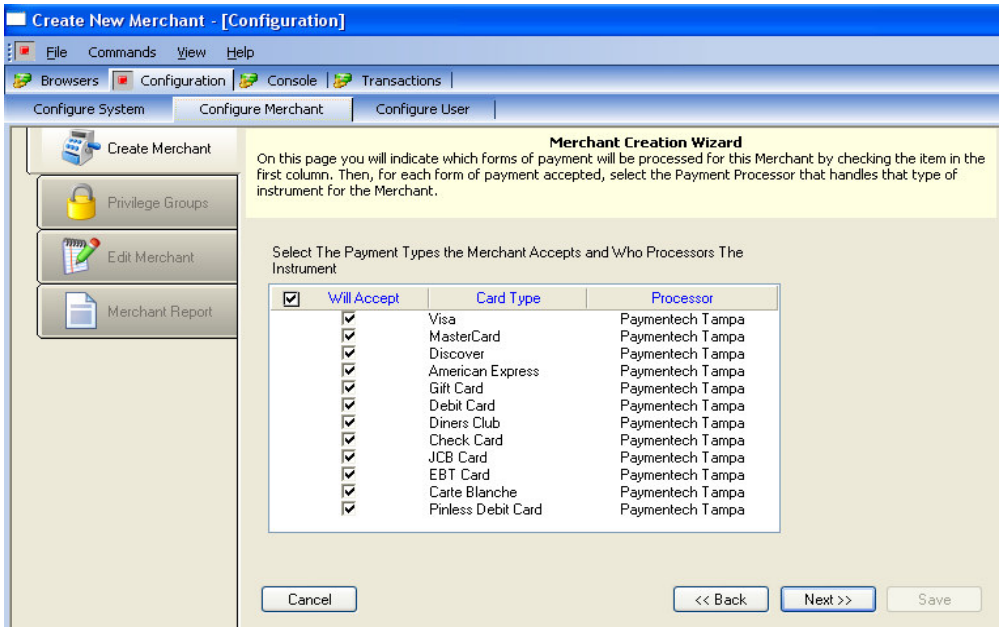
Step 4

- Enter your Merchant Parameters that were provided by the Payment Processor company
- Click "Next"



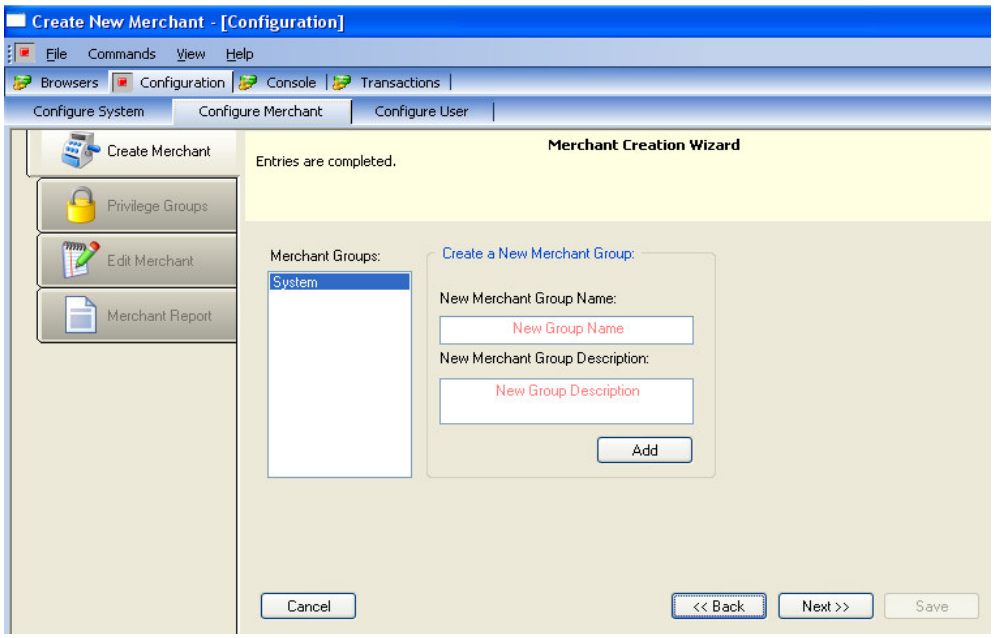
Step 5

- Select the merchant's accepted payment type
- Click "Next"



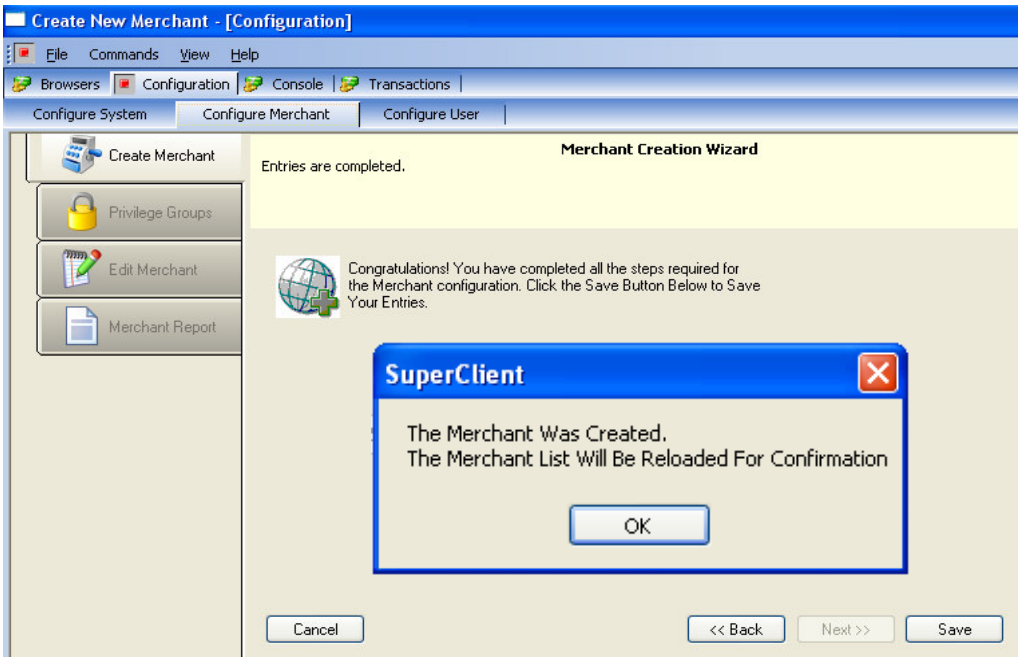
Step 6

- Create a "New Merchant Group" (optional)
- Select the Merchant Groups the merchant will be associated with
- Click "Next"

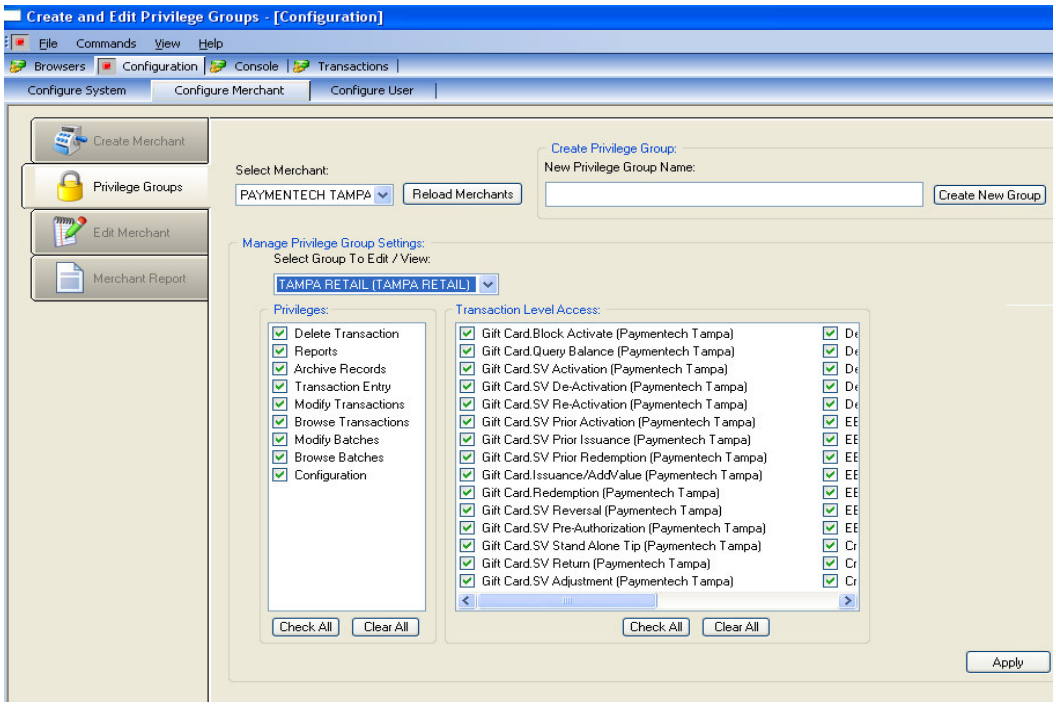


Step 7

- Click “Save”
- Click “Ok” when new merchant has been created



Privilege Groups



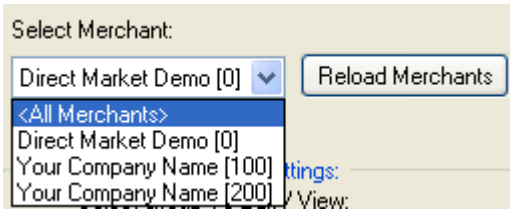
After you have created your merchants within TranScend™, you will need to set up the privilege groups for those merchants. Privilege Groups are an important security feature within TranScend™ as it allows the system administrator to strictly define and restrict which users have access to specific system functions.

The screen shown below will allow you to create and define the system functions associated with privilege groups. A privilege group must be created when you only want specific users to have specific permissions. For example, you want them to be able to browse transactions that are pending settlement but not be able to delete or modify the transactions.

Create privilege Groups

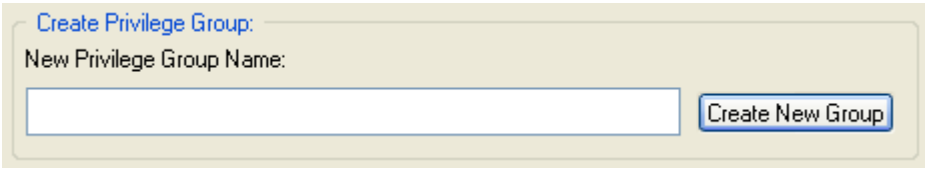
Step 1

- Click the "Reload Merchants" button to display all Merchants
- Select a Merchant from the Merchant drop-list



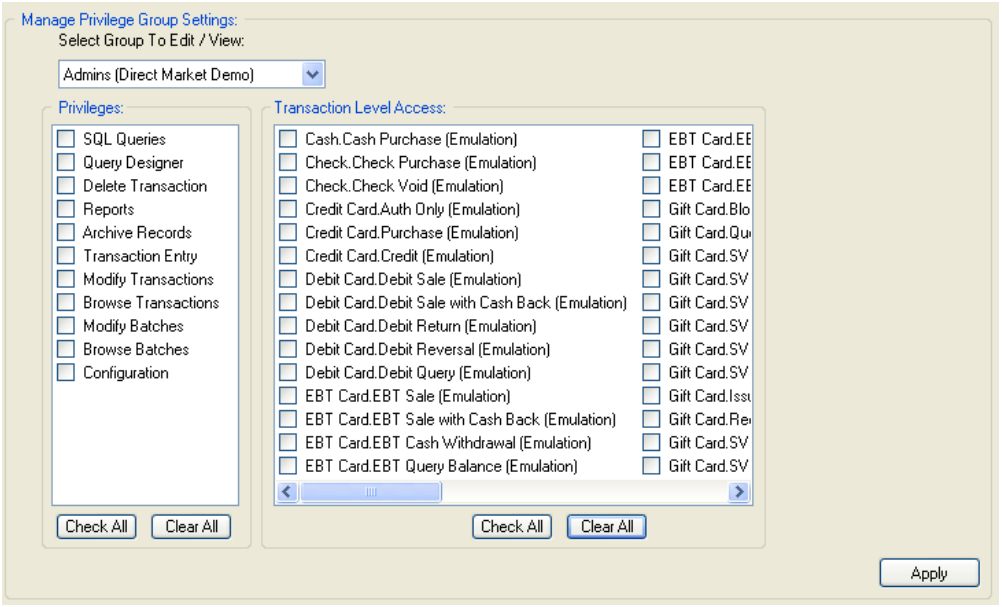
Step 2

- Under "New Privilege Group Name" type the name for the New Privilege group
- Click "Create New Group" button



Step 3

- Select the Privilege Group you wish to set from the "Select Group to Edit/View" drop-list
- Check the boxes from the list that you want members of that group to have
- Click "Apply" to save your settings you made for the Privilege Group



Edit Privilege Group

Step 1

- Click the “Reload Merchants” button to display all Merchants
- Select a Merchant from the Merchant drop-list

Step 2

- Select the Privilege Group you wish to set from the “Select Group to Edit/View” drop-list
- Check the boxes from the list that you want members of that group to have
- Click “Apply” to save your settings you made for the Privilege Group

Edit Merchant

This screen will allow you to edit existing merchant on the system and make any necessary updates or corrections to already existing merchant configurations.

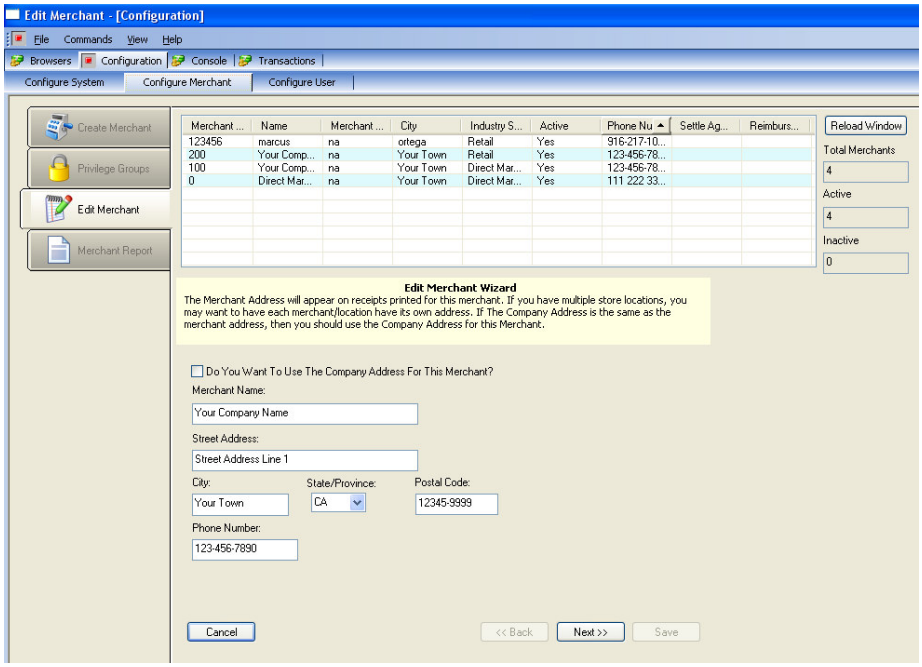
In general the edit merchant function uses the same wizard screens that were used to create a merchant, with the main difference being that wherever possible, the entries in the screens are pre-filled with the settings that are already Comment for the merchant whose settings are being changed.

Therefore, to edit a merchant, all that needs to be done is to double-click the list showing all the merchants already configured in the system. Once this action is performed, the selected merchant's settings will be used to pre-fill the settings in each of the wizard screens.

Therefore, to edit the settings for a merchant, simply complete each of these screens exactly as you would if you were using the merchant creation wizard, only you have the opportunity to change any setting on each of the screens in order to make the necessary changes.

Step 1

- Click the "Reload Window" button to display all merchants
- Double-Click a Merchant record to edit



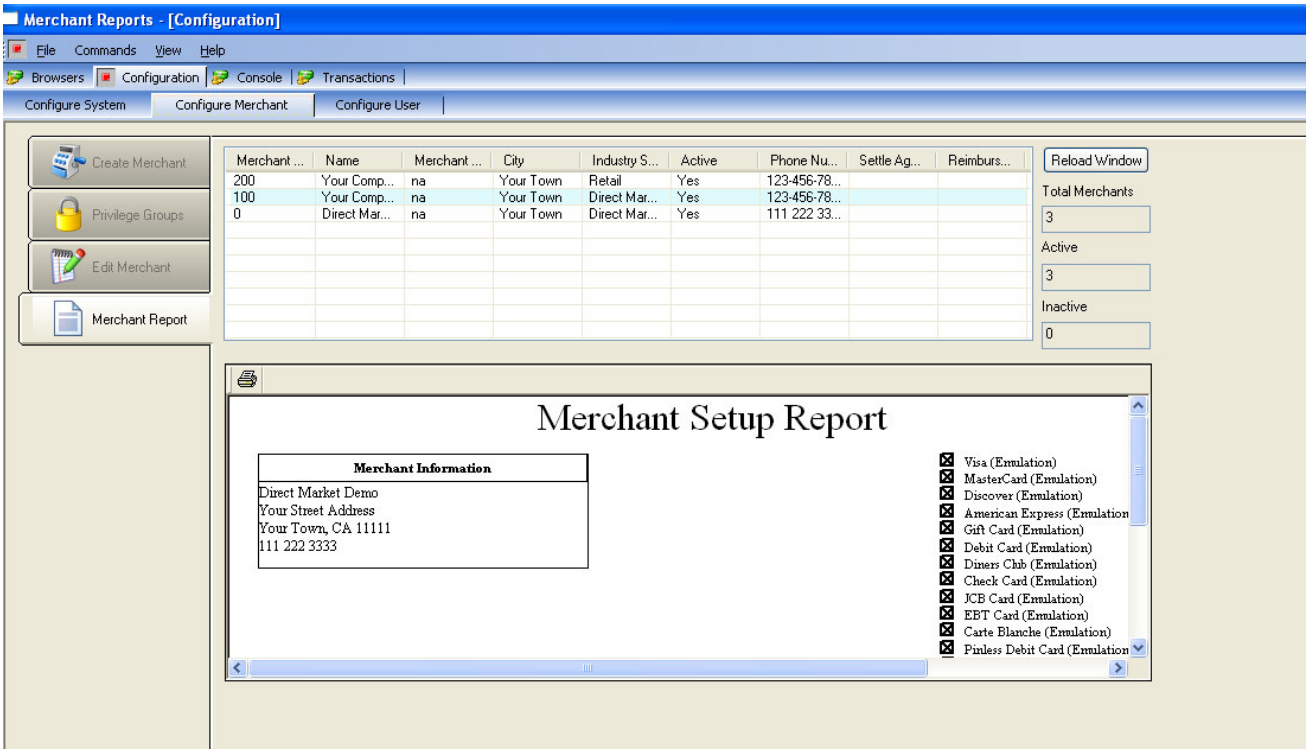
Step 2

- Make any changes that are appropriate
- Click the "Save" button to save any changed settings

Merchant Report

This screen will allow you to quickly view a summary of the merchants configured on your system. You can also print a Merchant Report if desired.

- Click the "Reload Window" button to display all merchants
- Double-Click the Merchant making the Merchant's settings to appear in the Merchant Setup Report window



Configure User and User Report Information

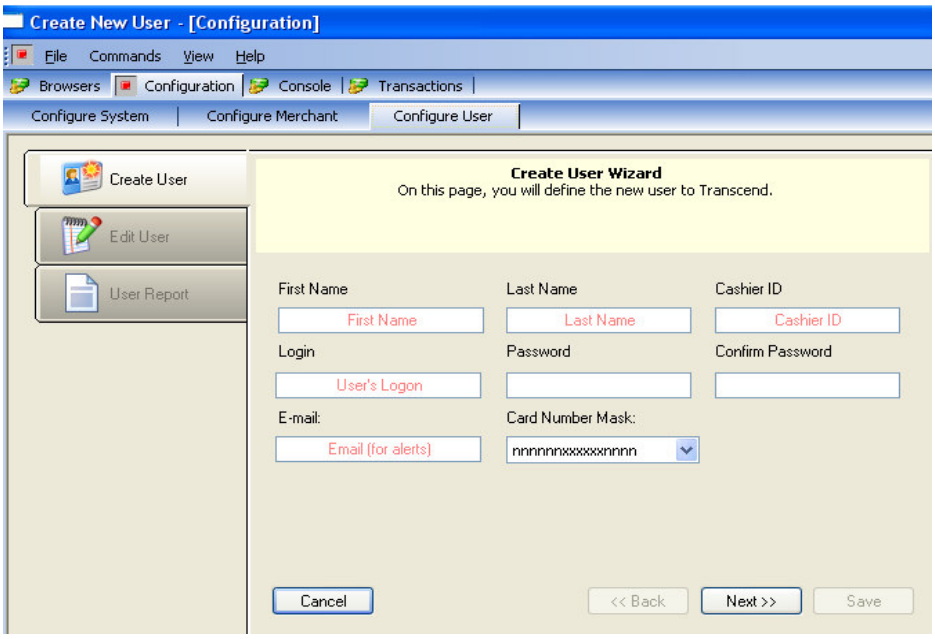
Configure Users

Create User

TranScend™ allows you to create users for user that will be interacting with the system. Each user can be affiliated with a set of functions that are assigned to the privilege group(s) that the user is associated with. This is a security feature of the TranScend™ system. As such, any user's access to system functions should be limited to only those that would be required by them to perform their job functions. The series of illustrated instructions that follow provide you with the information required to create users for the TranScend™ system.

Step 1

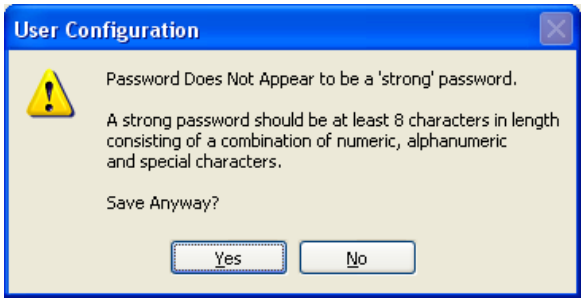
- Login to the Transcend client utility
- Click on the "Configuration" tab
- Click on the "Configure User" tab
- Click on the "Create User" tab

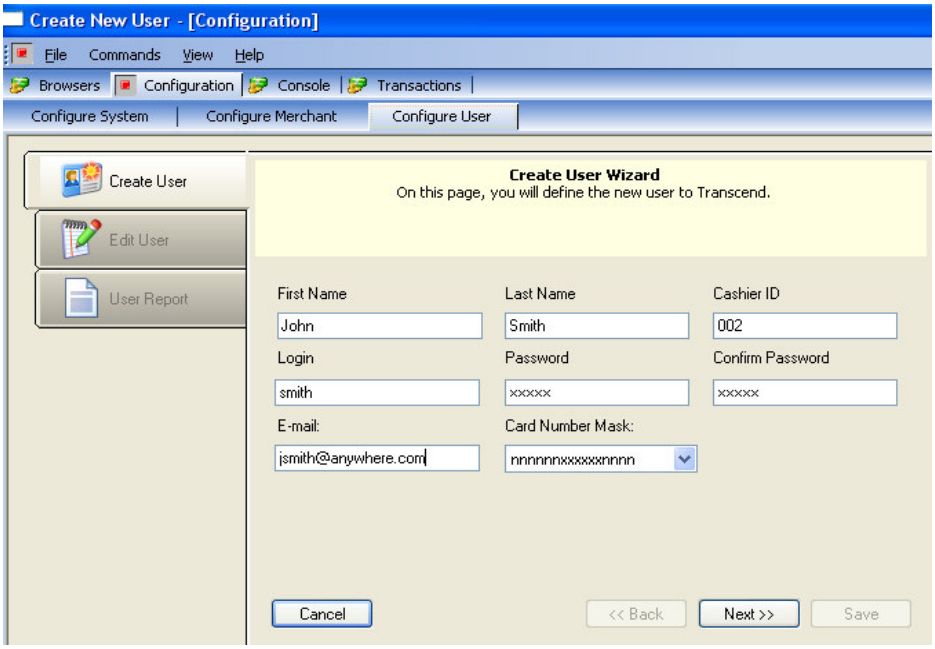


Step 2

- Enter the new user's information
- Click "Next"

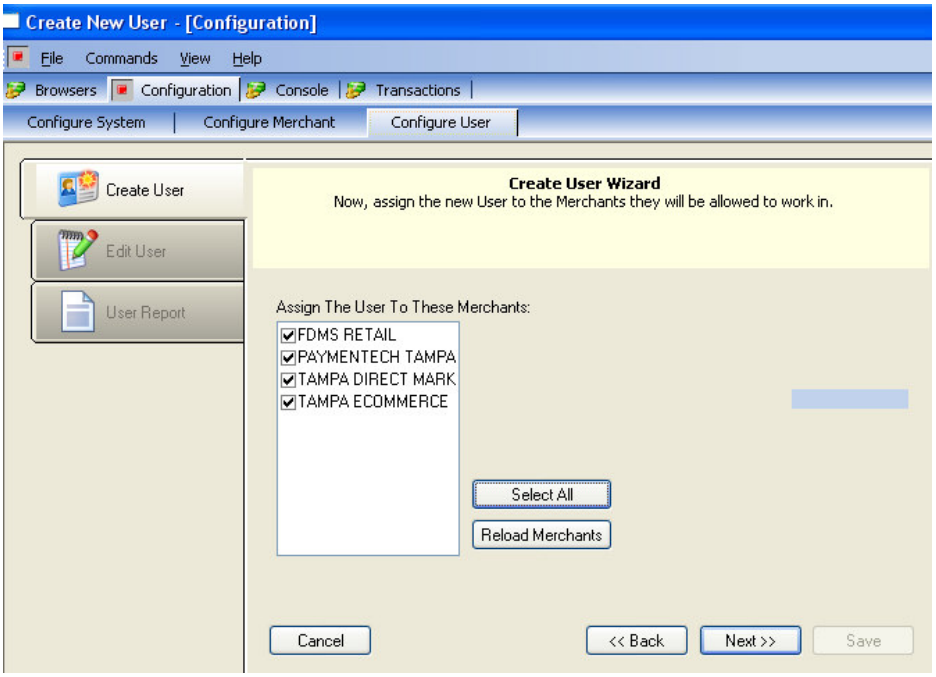
NOTE: If the password entered is not 8 characters long or not unique you will get this message:





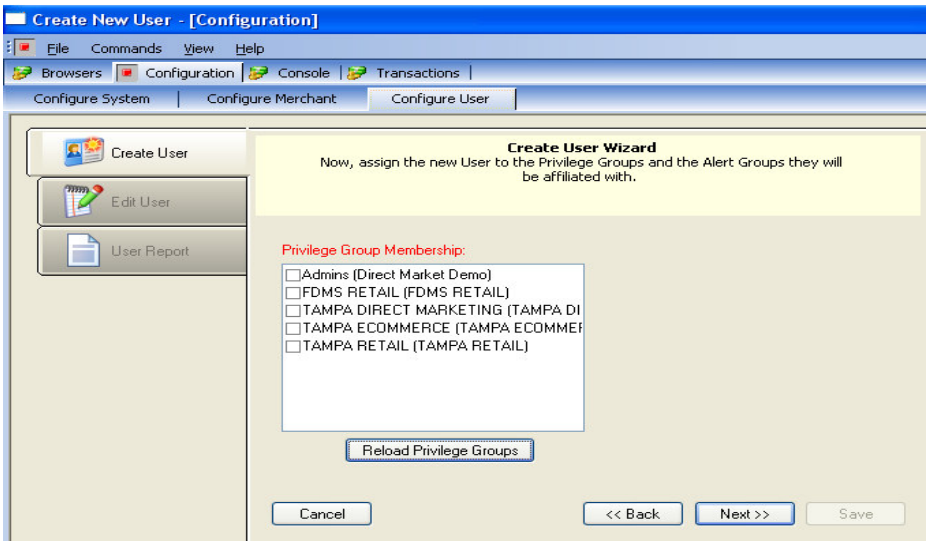
Step 3

- Pick your Merchant(s) that this user will be granted access to
- Click “next”



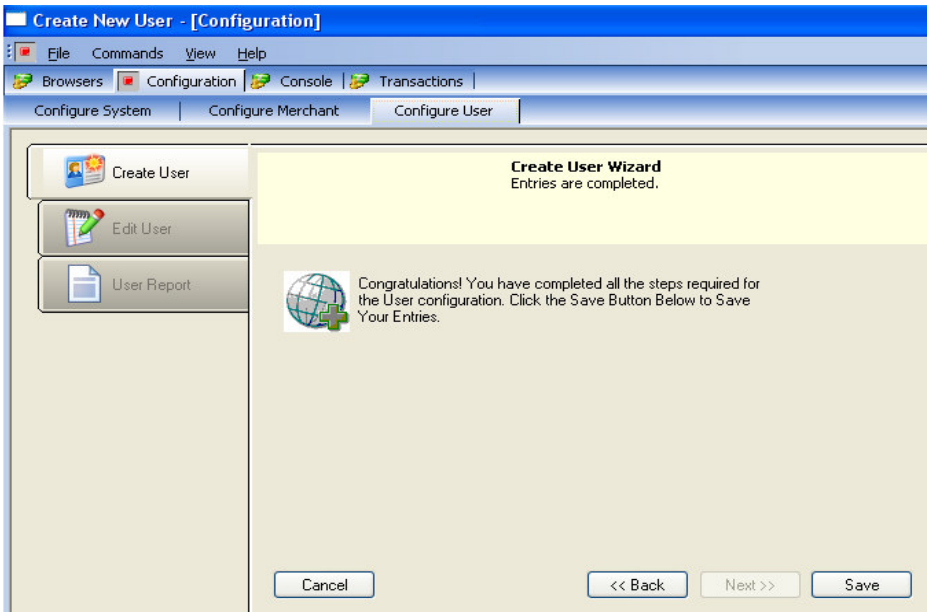
Step 4

- Pick your Privilege Group(s) that this user will be associated with
- Click “Next”



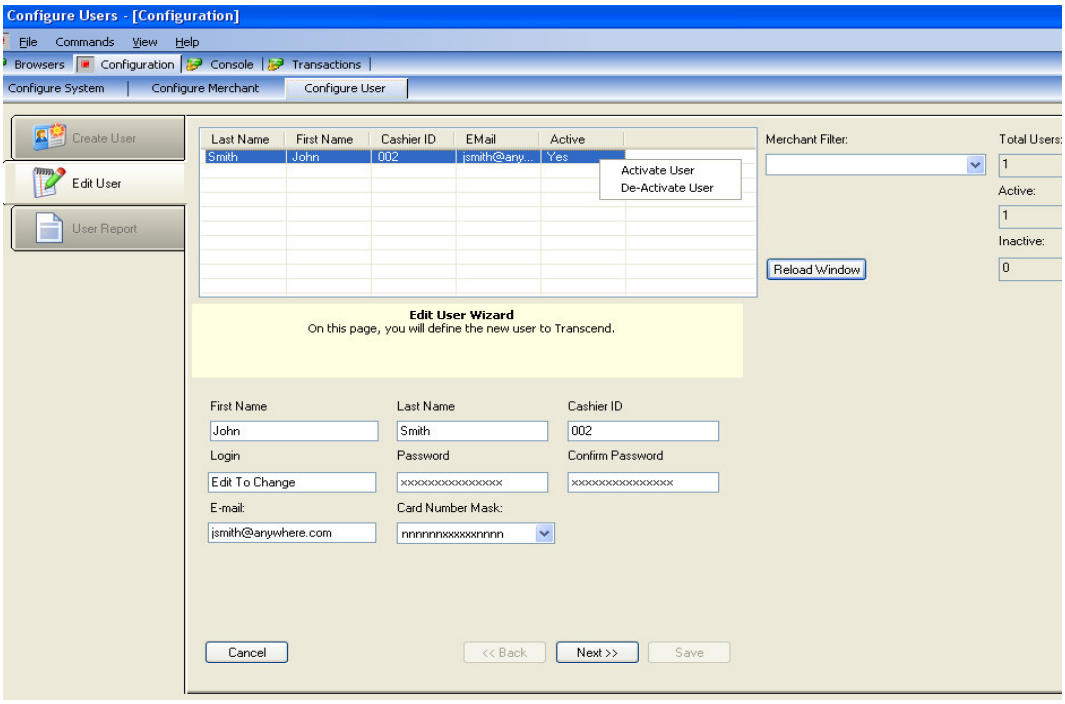
Step 5

- Click “ Save”



De-Activating Users

- Login to the TranScend™ client utility
- Select the “Configuration” tab
- Select the “Configure User” tab
- Select the “Edit User” tab
- If the User List is empty, click the “Reload Window” button
- Right-Click on the record for the user that should be deactivated
- Select the “De-Activate User” menu Command



Editing Users

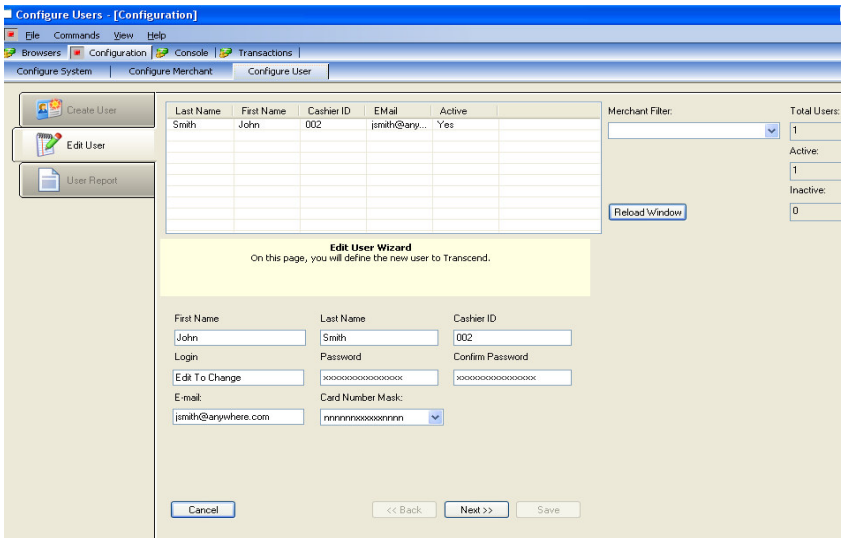
In general the edit user function uses the same wizard screens that were used to create a user, with the main difference being that wherever possible, the entries in the screens are pre-filled with the settings that are already Comment for the user whose settings are being changed.

Therefore, to edit a user, all that needs to be done is to “Double-Click” the list showing all the users already configured in the system. Once this action is performed, the selected user’s settings will be used to pre-fill the settings in each of the wizard screens.

Therefore, to edit the settings for a user, simply “step through” each of these screens exactly as you would if you were using the user creation wizard, only you have the opportunity to change any setting on each of the screens in order to make the necessary changes.

Step 1

- Login to the TranScend™ client utility
- Select the “Configuration” tab
- Select the “Configure User” tab
- Select the “Edit User” tab
- If the User List is empty, click the “Reload Window” button
- Double-Click on the user record that should be changed
- Click “Next”



Step 2

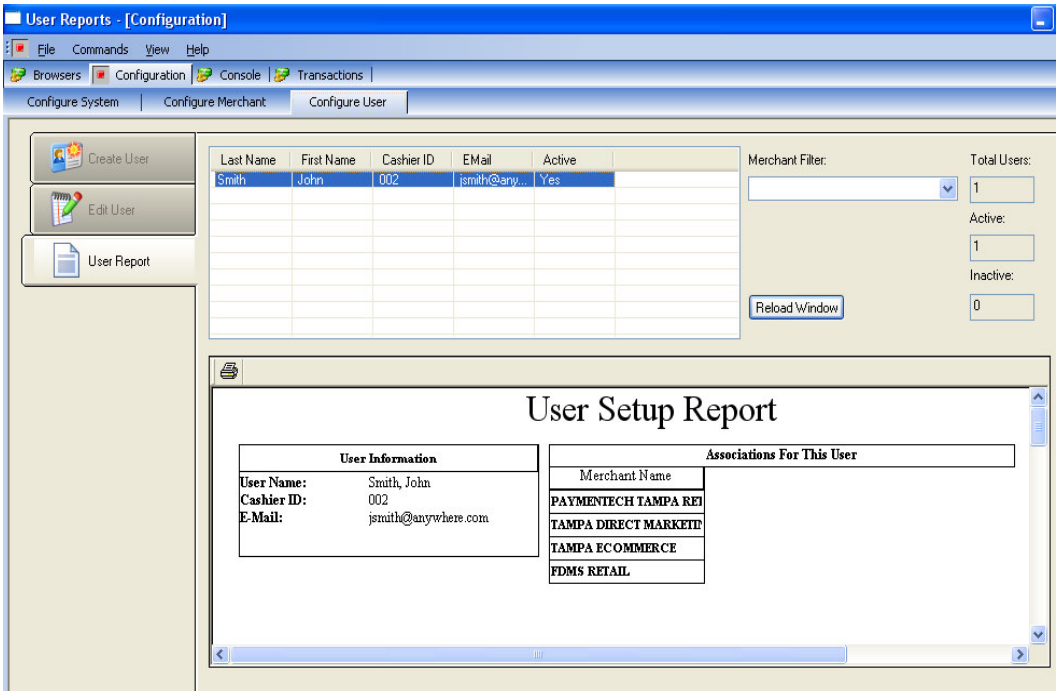
- Navigate through the Wizard Screens making any changes that are appropriate.
- Click the “Save” button at the end of the wizard to save your settings you made for the User

User Reports

This screen will allow you to quickly view a summary of the users configured on your system. You also have the option of printing the User Report from this screen.

Printing User Reports

- Click the "Reload Window" button to view users
- Double-Click the desired user to access their User Report
- Clicking on the  icon will allow you to print a hard copy of the User Report



Transactions Entries and Browsing Functions

Transactions

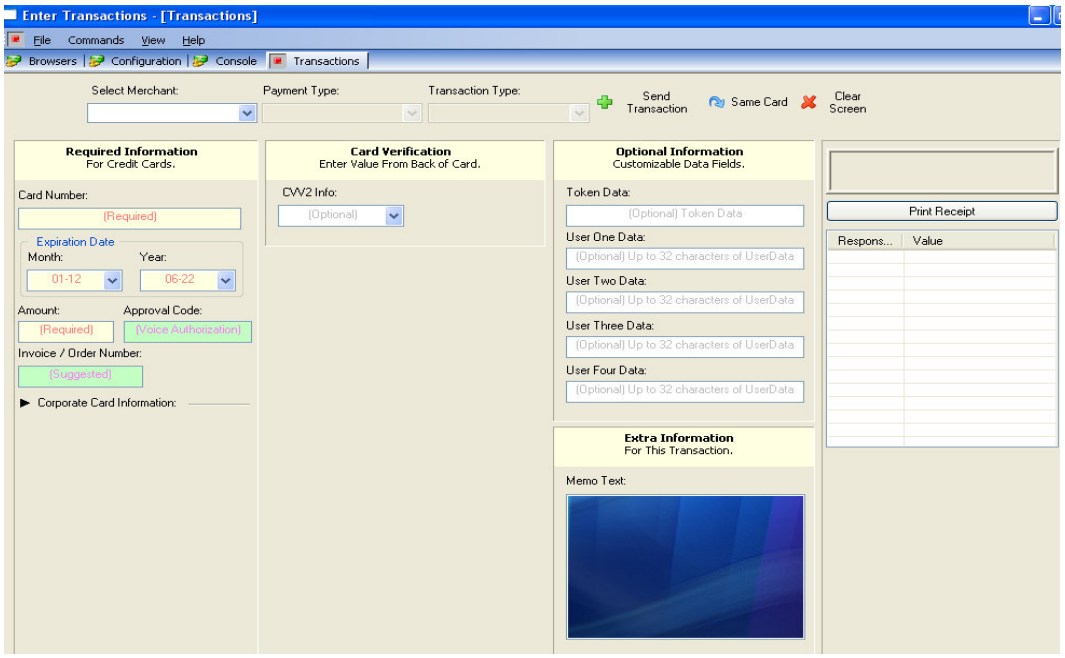
The transactions tab is one of several entry points for processing new transactions in TranScend™. This screen has been designed to accept several different types of payment. For example; credit cards, debit cards, EBT, and gift cards are all supported from this single screen. Supported payment types will be limited to your chosen payment processor and the merchant configuration.

The transactions tab has also been designed to support the extra data elements as may be required for the various market segments: Retail, Direct Marketing and E-Commerce. Examples of each of these variants of the transaction entry screen are shown immediately below:

Transaction Screen Panels

The transaction screen is broken into 6 sections (called panels). Each Panel is outlined in its own area on the screen. Each panel also has a title banner above it.

- **Required Information Panel**- in this section the card holder's credit card information is entered. The yellow fields are required before the transaction can be processed. The green and white fields are optional
- **Card Verification Panel-** you enter the CVV2 information in this section
- **Optional Retail Information Panel-** specific card holder information is entered in this section. For example, card holder name and address.
- **Optional information Panel-** this section is where you would enter additional information about the transaction being processed. For example, more detail about the transaction or person/register processing the transaction.
- **Extra Information Panel-** allows you to attach a memo to the transaction. This is essential if there are any special instructions related to the transaction.
- **Status Panel-** located on the far right, this section will show you the status of the transaction after it is submitted. Printing a receipt is also available in this section.



Retail Transaction Entry

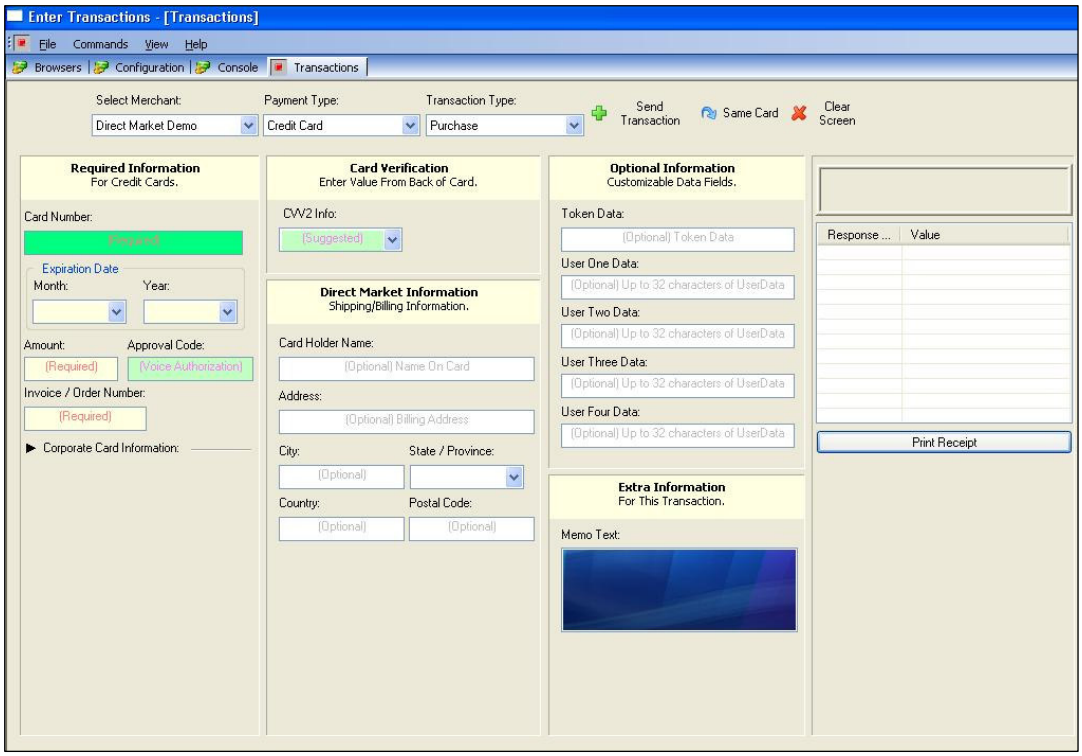
With the Retail panel, all data fields are optional. Even though they are optional, it is beneficial to enter values in the CVV and Postal Code fields for non-swiped transactions.

Direct Marketing Transaction Entry

With the Direct Marketing Transaction Entry, all data fields are optional. Although these fields are optional it is advantageous to enter CVV and Postal Code fields for no-swiped transactions.

E-Commerce Transaction Entry

Unlike the Retail and Direct Marketing Transactions, E-Commerce Transaction Entries require many data fields. But like the others, the CVV field is optional, keep in mind it is valuable to enter the values in the field.

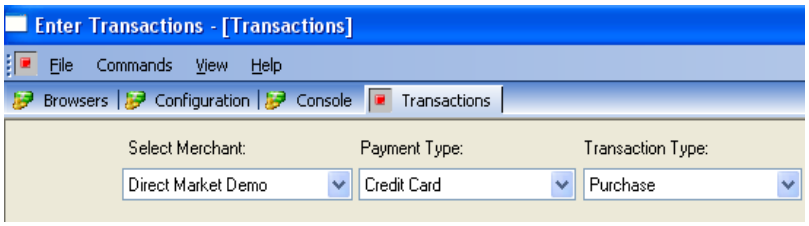


Transaction Entry

Processing a new transaction and taking a closer look at the transaction window and its various sections.

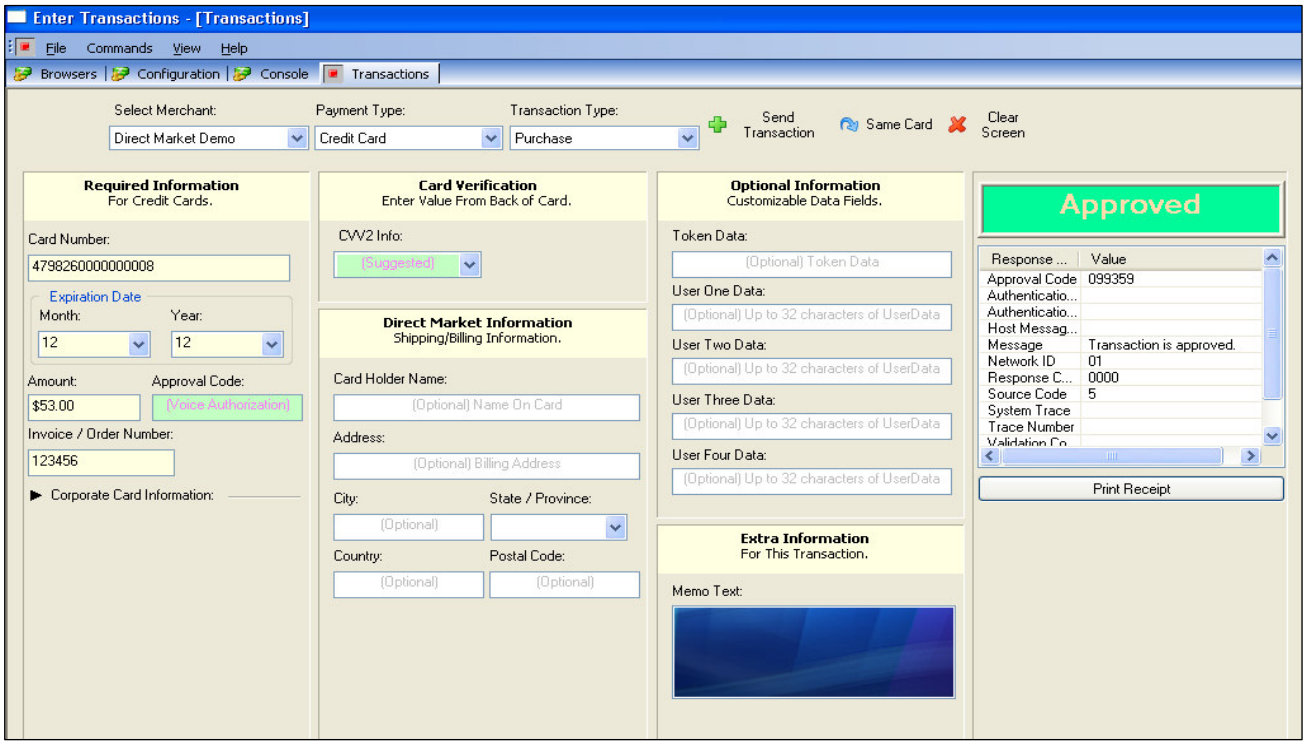
Step 1

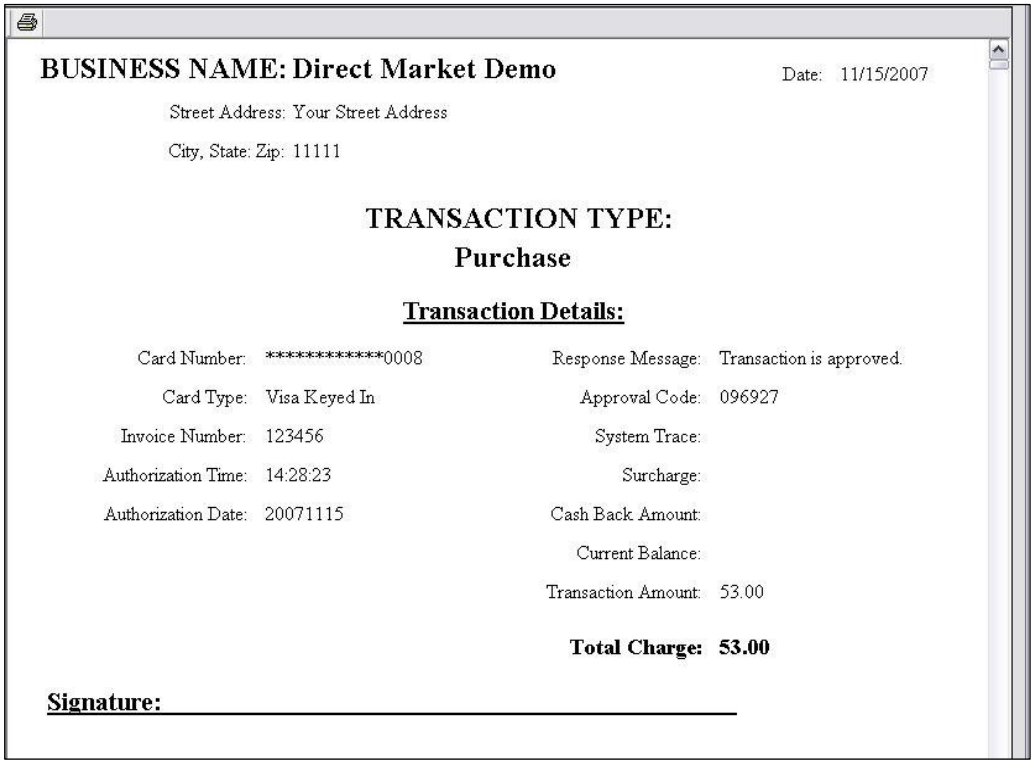
- Select a merchant from the "Select Merchant" drop down menu.
- Select a payment type from the "Payment Type" drop down menu.
- Select the type of transaction from the "Transaction Type" drop down menu.



Step 2

- Enter card holder's credit card information (card number and expiration date).
- Enter amount to be charged
- Click on "Send Transaction" to process the transaction





BUSINESS NAME: Direct Market Demo Date: 11/15/2007

Street Address: Your Street Address

City, State: Zip: 11111

TRANSACTION TYPE:
Purchase

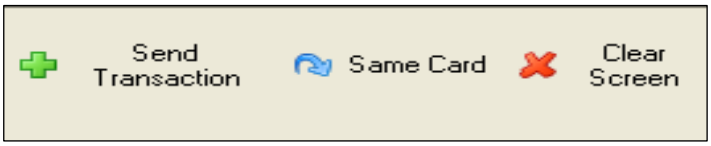
Transaction Details:

Card Number:	**********0008	Response Message:	Transaction is approved.
Card Type:	Visa Keyed In	Approval Code:	096927
Invoice Number:	123456	System Trace:	
Authorization Time:	14:28:23	Surcharge:	
Authorization Date:	20071115	Cash Back Amount:	
		Current Balance:	
		Transaction Amount:	53.00
		Total Charge:	**53.00**

Signature: _____

The example above shows a card approval from the payment processor in the status panel area. You are also given the option to "Print Receipt" by clicking on the selecting the button anytime that the transaction data is still displayed in the results summary panel. A sample receipt is shown to the left. Note that if your organization requires customized receipts, you may want to discuss these options with your sales representative.

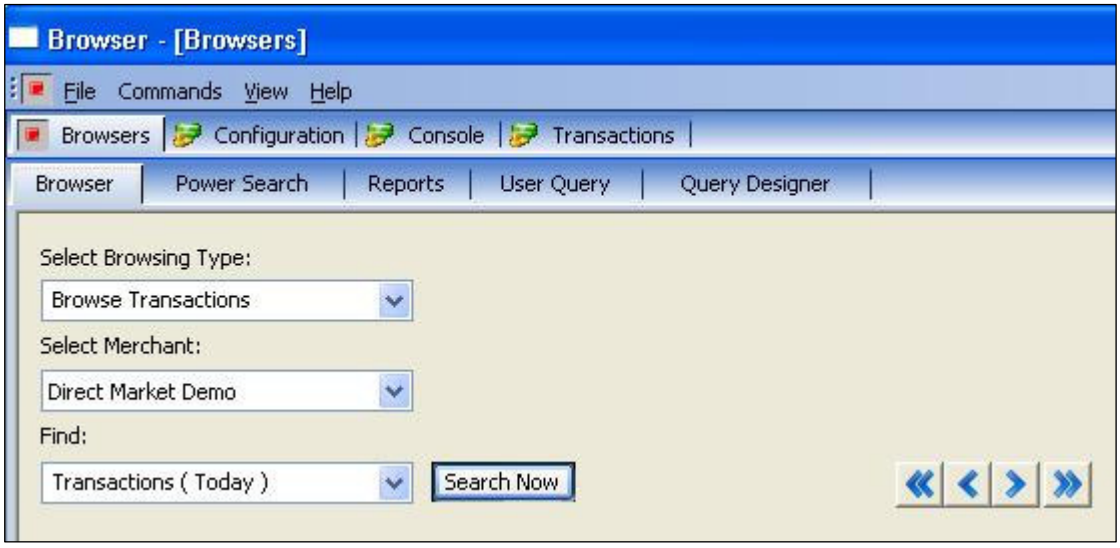
If you need to resubmit another transaction from the same card holder, clicking on the “Same Card” button will retain the card holder’s information from the previous transaction. Only a new amount is required to be charged, and then click on “Send Transaction”.



If a mistake is made at any point or you want to start the transaction over, click on the “Clear Screen” button to reset the screen.

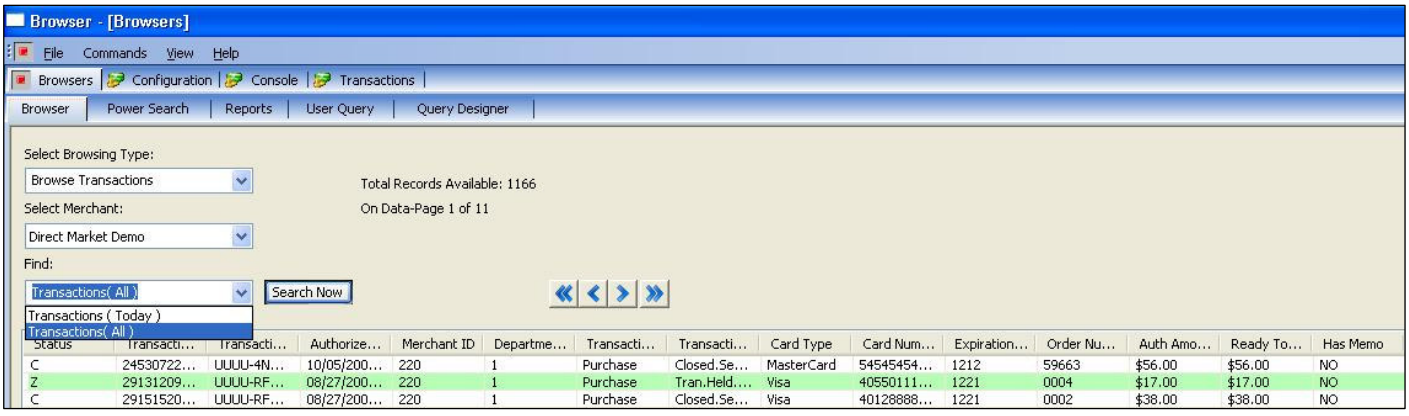
Browsing Tools

The Browse Tab will enable you to view the Transactions and Batches that are in your TranScend™ database. You will have the option to Browse Transactions or Browse Batches and sort by Merchant and then selecting the option under Find.

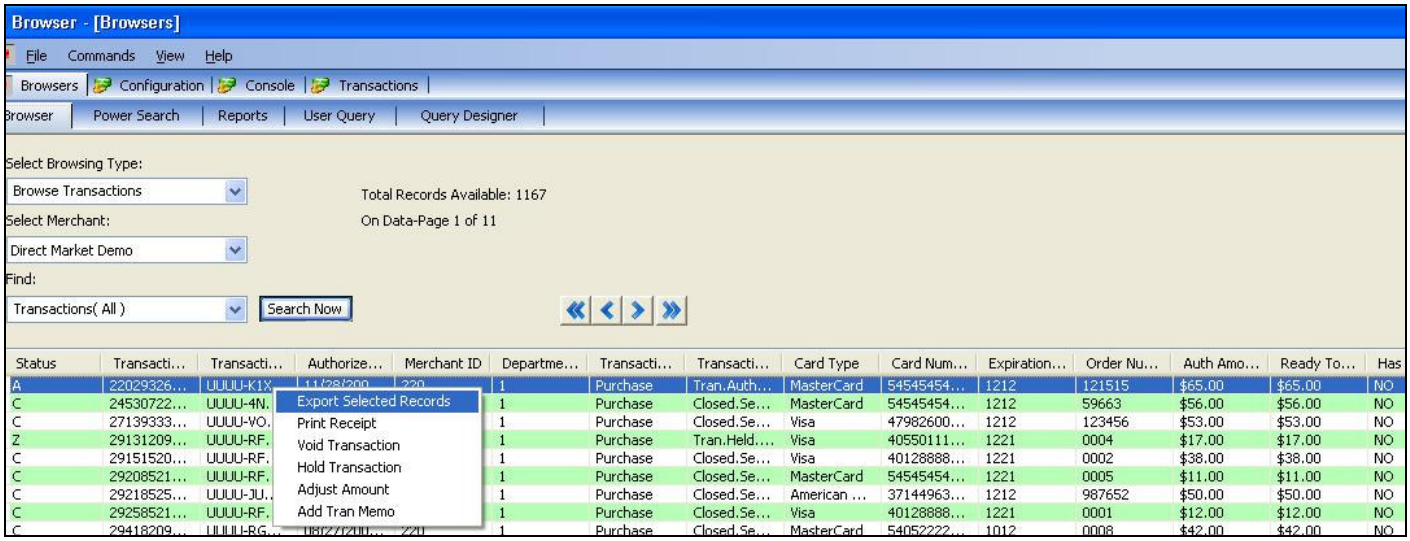


Browsing Transactions

In the Browse Transaction screen you will be able to view your Transactions based on merchant, also in the Find option you will be able to select the retrieval of all records or only today's records. You can click on the column headers on the top of the list to sort by any column in the list. If you want to perform more than one column as sorting criteria, simply hold down the CTRL key while you click any additional columns to included in the overall sub-sorted list displays. You can sort on as many columns as you'd like with this feature.



Transaction Management and Context Menus



All transaction management functions in the TranScend™ client are available through context menus on the browse screens. In some cases, the commands available in the menu will vary based on the transaction status. Accordingly, the sections that follow will illustrate each of these conditions.

Export Selected Records

Selection of this command will allow the currently selected records in the list to be exported from the client and saved into a file. The currently supported file formats are: Excel Worksheet and Comma Separated Values (CSV). Since File Dialogs are commonly understood, no image is provided for that screen.

Print Receipt

Selection of this command will cause a *Reprinted* Receipt to be displayed for the selected transaction.

You can see that Reprinted receipts will show that word. This is so that one can immediately be able to recognize these kinds of receipts from the original ones produced by the system.

Void Transaction

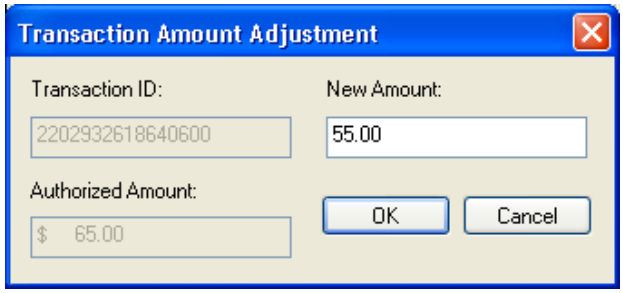
Selection of this command will cause the transaction to not be settled. This command should be used to "reverse" a transaction that has not yet been settled (deposited). Since this is an irreversible operation, you will have to confirm that this action should be performed with the message box that will be shown.

Hold Transaction

Selection of this command will prevent the transaction from being settled until its status is changed again to a "Settle Ready" status. This command should be used to put a transaction into a "suspended state" while some research is being done or when the customer's goods have not yet been delivered (in the case of an E-Commerce or MOTO merchant type).

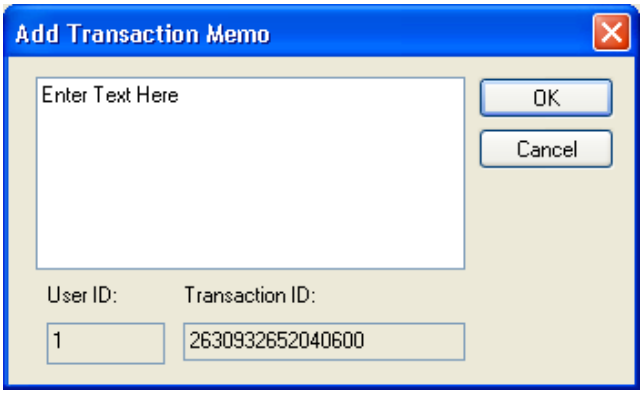
Adjust Transaction

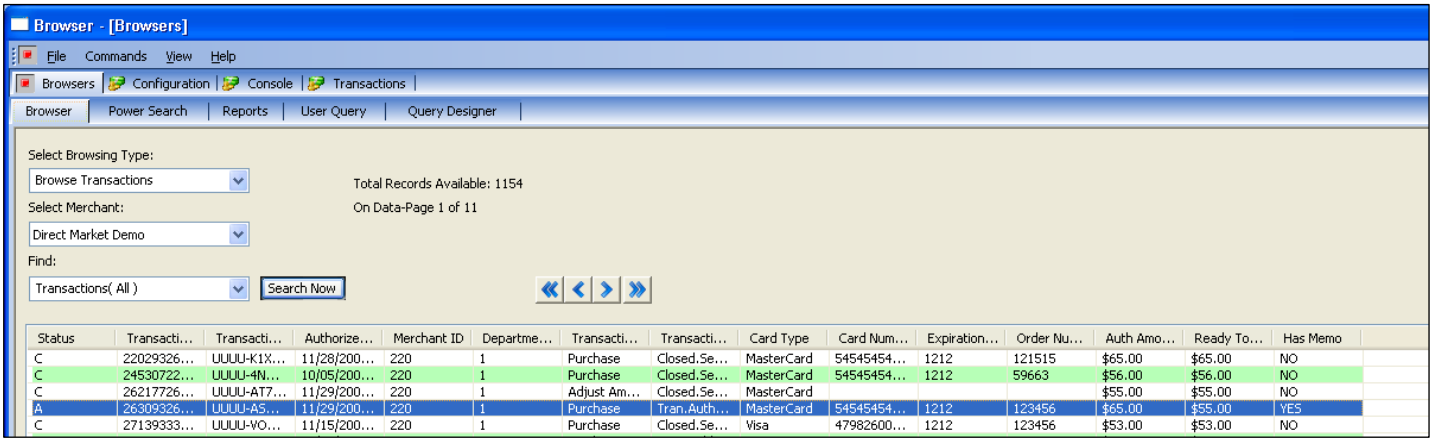
Selection of this command will present the dialog shown at the right. Completion of this screen will allow the amount of the transaction to be altered. Note, that this screen can only be used to make the amount less (never more). This command should be used whenever the final settlement amount should be lower than the originally authorized amount. One case where this may become needed is for a MOTO or Ecommerce merchant where has only been partially delivered.



Add Transaction Memo

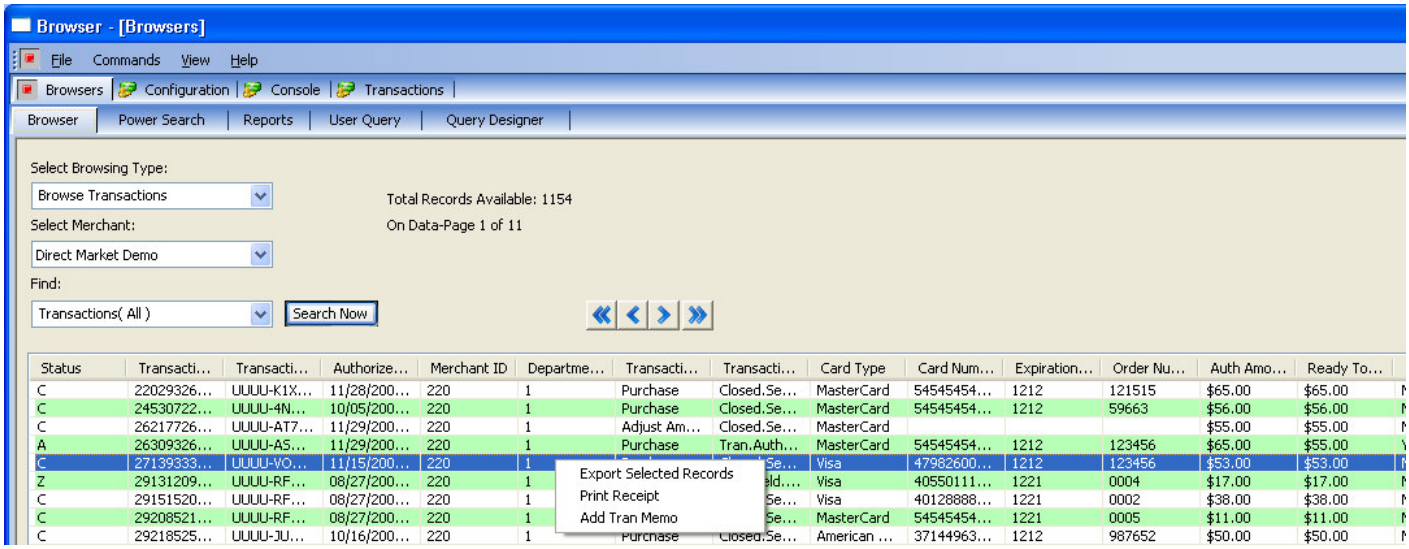
Selection of this command will allow additional notations to be stored with the transaction. This feature can be useful for tracking various types of information that should be associated with the transaction. These notations can be displayed at any time. If you examine the image below, you will see that transactions that have Memos associated with them will have the word YES in the final column of the list.





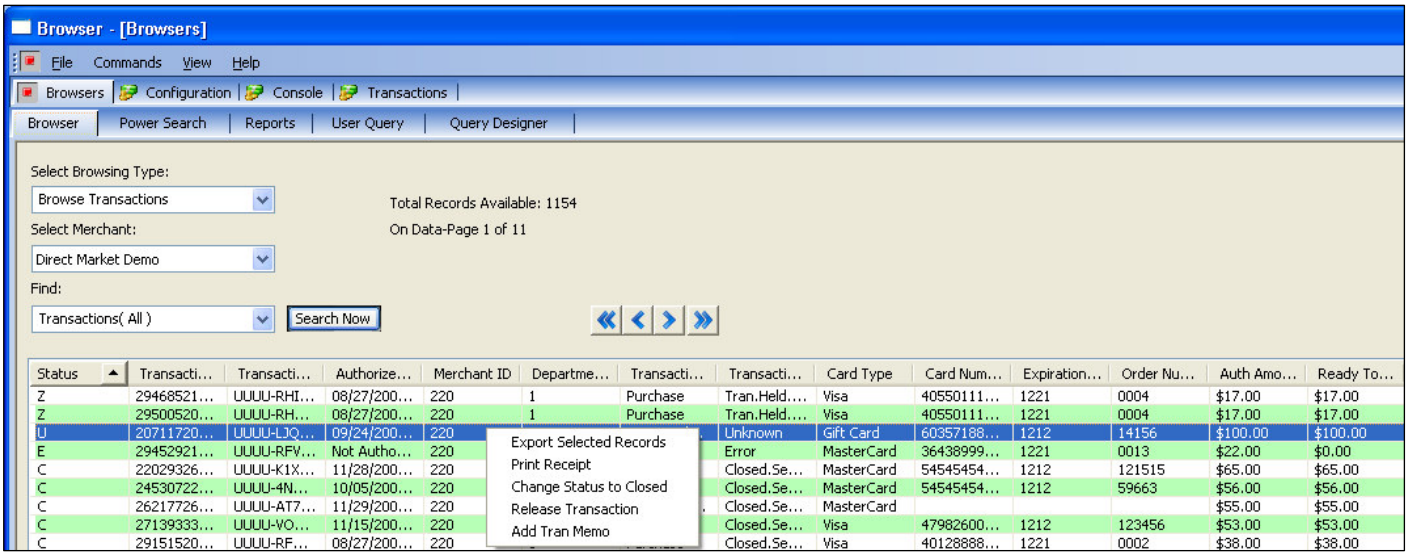
Menu Commands for Closed Transactions

In the image shown below, you can see that there are less commands available when transactions have been closed.



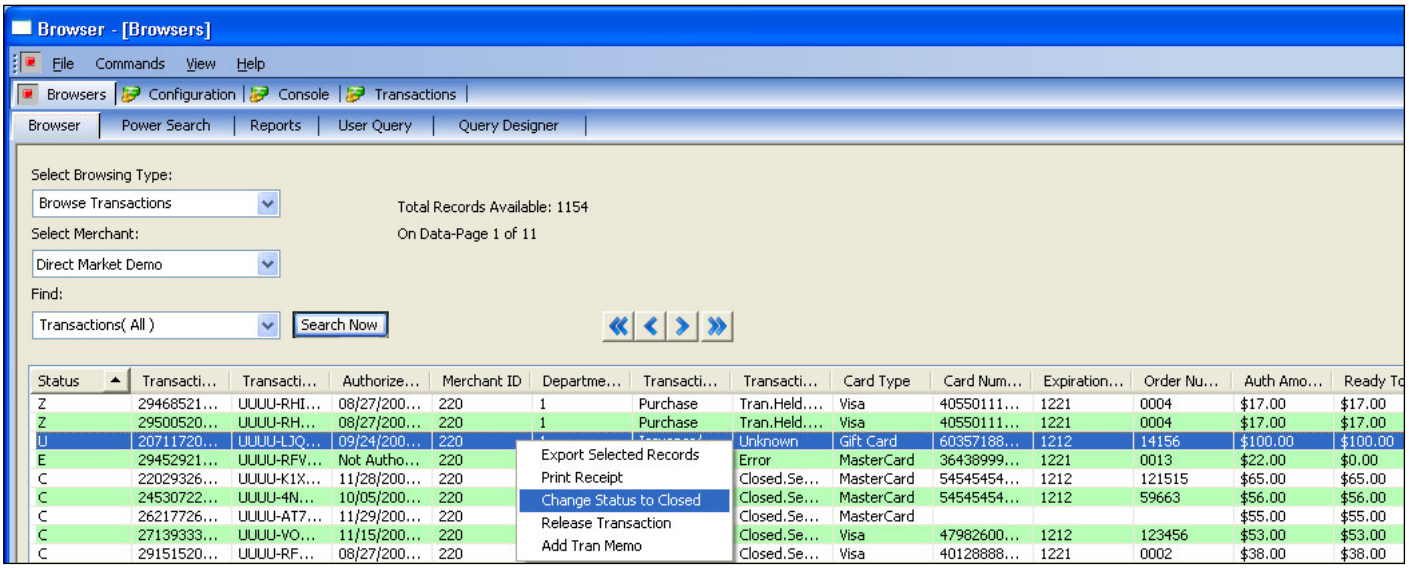
Menu Commands for Transactions that are "On-Hold"

Transactions can be put on hold due to AVS, CVV system holds, or from manually placing a transaction on hold. In the image shown below, you can see that there are additional commands available for transactions that are on hold. The first new command shown below is the "Release Transaction" command. Selection of this command will remove the hold status on the transaction and will allow the transaction to be included in the next settlement job. The next new command is the "Change Status to Closed" command. Selection of this command will close the transaction. **Caution**: Closed Transactions *will not be settled*.



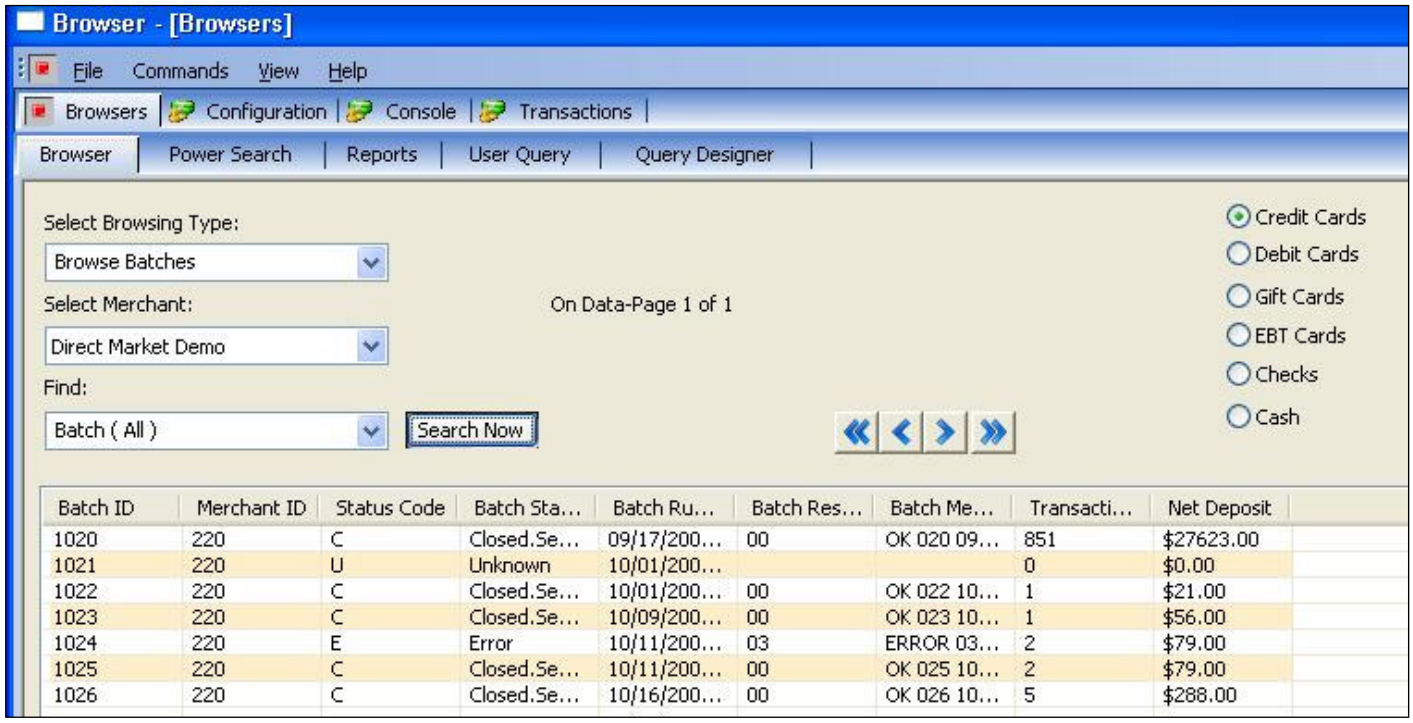
Menu Commands for Transactions in an Unknown-Status

The image below shows the transactions that are available when transactions are in an Unknown status. Each of these commands has been explained in previous sections.



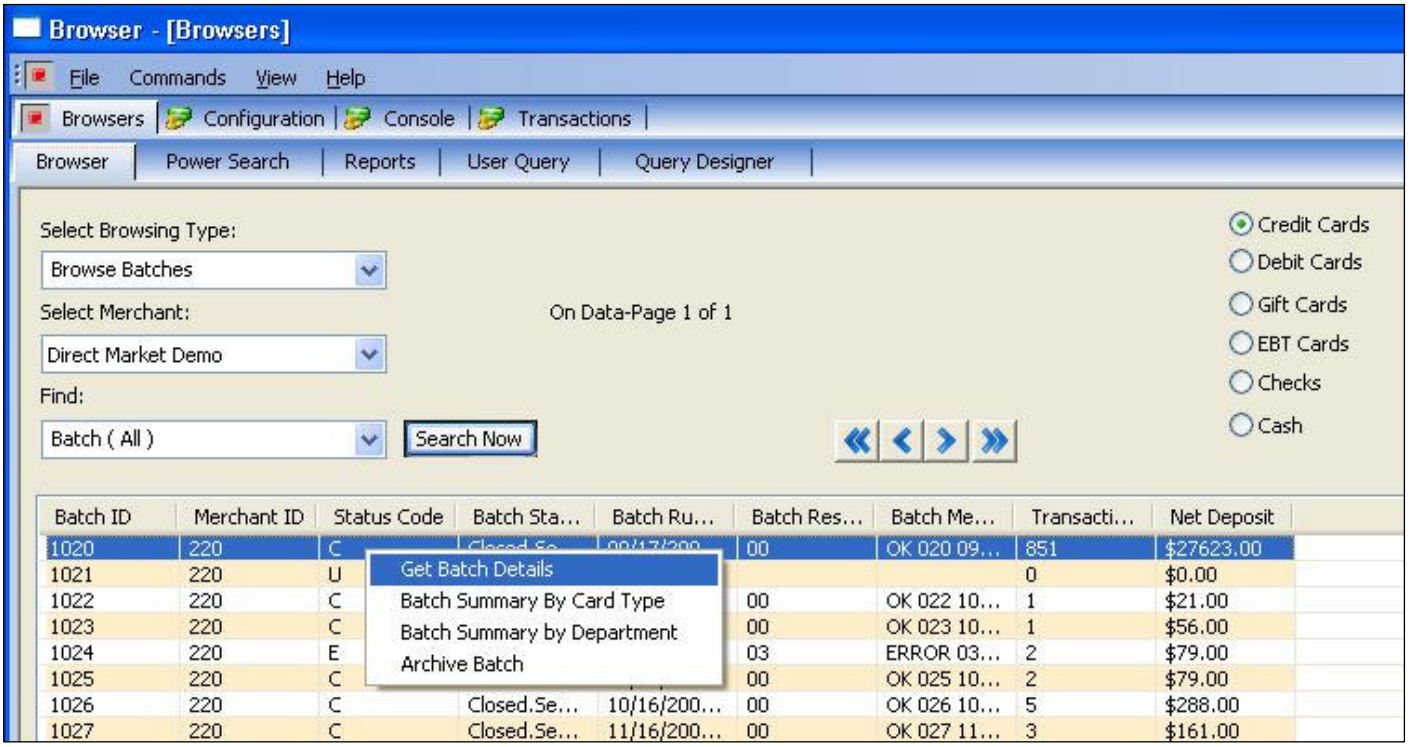
Browse Batches

The image above shows the “Browse Batches” window. Notice that the column headings are different than those in the “Browse Transactions” window and the commands menu has different options. The same sorting feature that was mentioned above is available for this list as well.



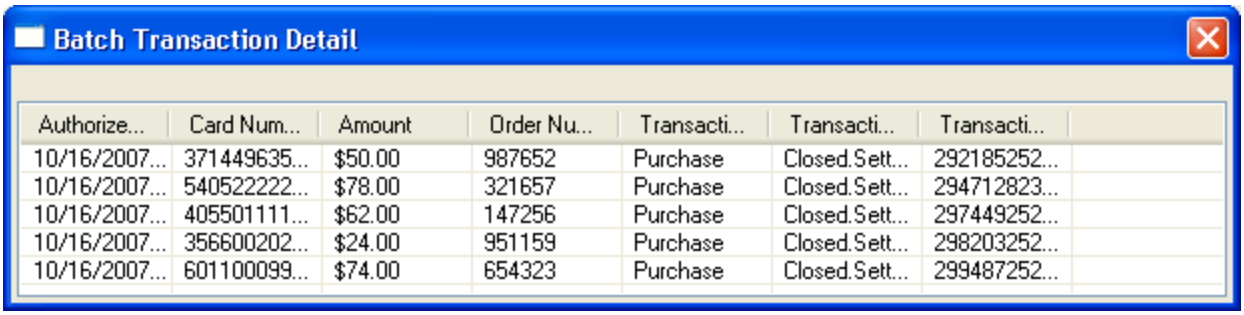
Batch Management And Context Menus

The image shown immediately below shows the commands that can be performed against Settlement Batches with the TranScend™ client program.



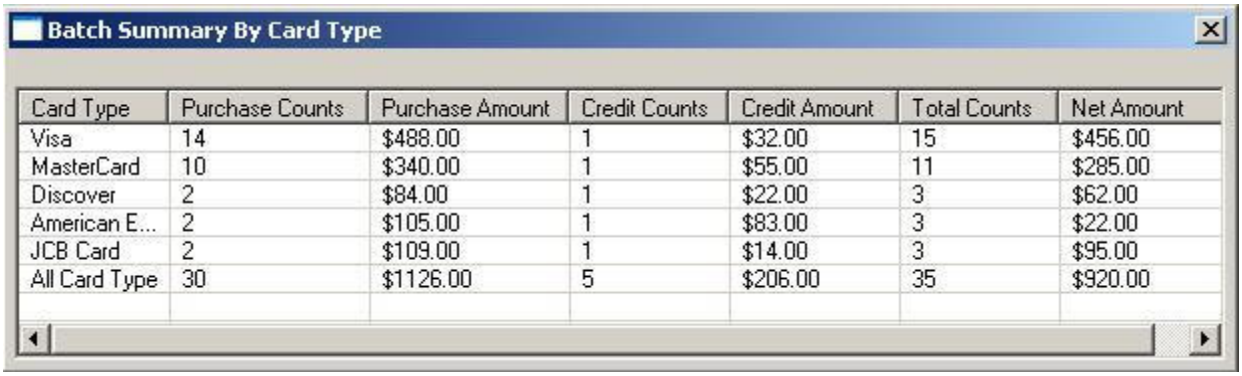
Get Batch Details

The image below shows the dialog that is displayed when the “Get Batch Details” command is executed. This window shows a detailed list of the transactions that are included within the selected batch. This dialog can be resized in order to show the number of records desired. This command is available for batches that are closed or are marked as having an error.



Batch Summary by Card Type

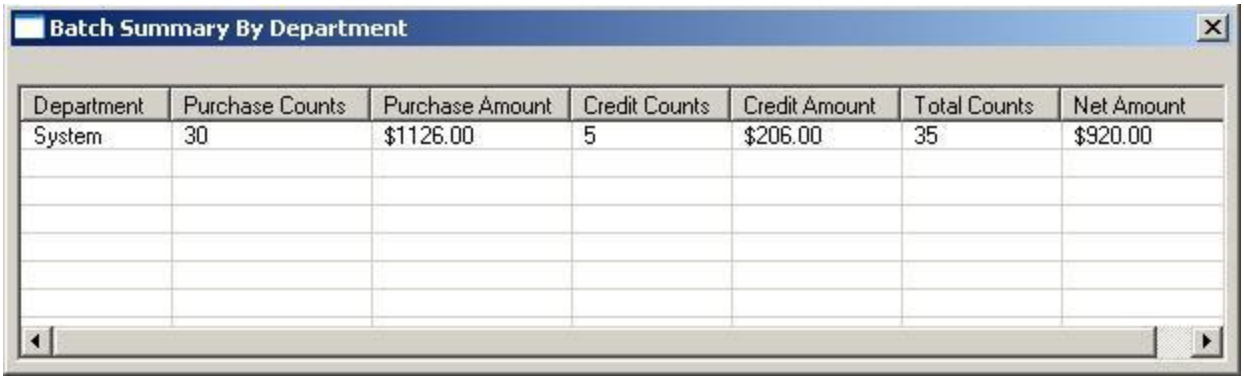
The image below shows another way that batch details can be summarized. Selection of this command will cause a total to be calculated for each card and transaction type contained in the batch. These sub-totals will be shown on the display window presented.



Card Type	Purchase Counts	Purchase Amount	Credit Counts	Credit Amount	Total Counts	Net Amount
Visa	14	$488.00	1	$32.00	15	$456.00
MasterCard	10	$340.00	1	$55.00	11	$285.00
Discover	2	$84.00	1	$22.00	3	$62.00
American E...	2	$105.00	1	$83.00	3	$22.00
JCB Card	2	$109.00	1	$14.00	3	$95.00
All Card Type	30	$1126.00	5	$206.00	35	$920.00

Batch Summary By Department

The image below shows another way that batch details can be summarized. Note that the departments feature is not currently utilized in the product. Due to this fact, this display shows only a single summary row that matches the batch display.



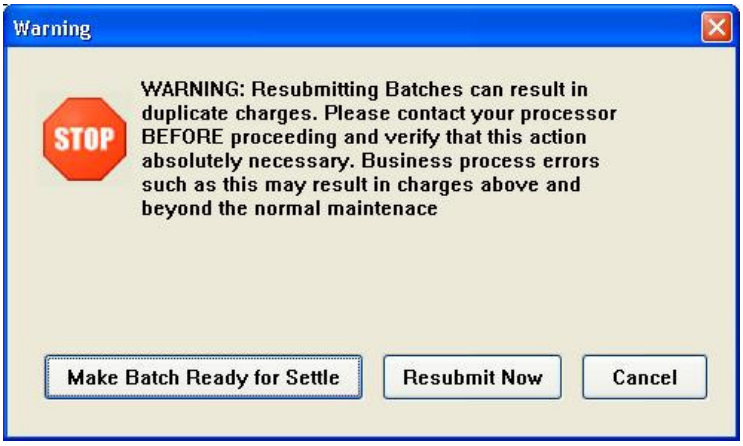
Department	Purchase Counts	Purchase Amount	Credit Counts	Credit Amount	Total Counts	Net Amount
System	30	$1126.00	5	$206.00	35	$920.00

Archive Batch

Selection of this command will copy the batch and all its detail records into the Archive database. It is important to note that once a batch has been archived it will no longer show up in the batch lists.

Resubmit Batch

On very rare occasions (and usually only under the direction of your processor) you may have to resubmit a batch. Selection of this command will cause the entire collection of transactions in the batch to be deposited again. Whenever this command is selected the warning message shown at the right will be displayed in order to point out the potential risks of performing this action. As was mentioned above, this command should only be selected under very exceptional circumstances.



Close Batch

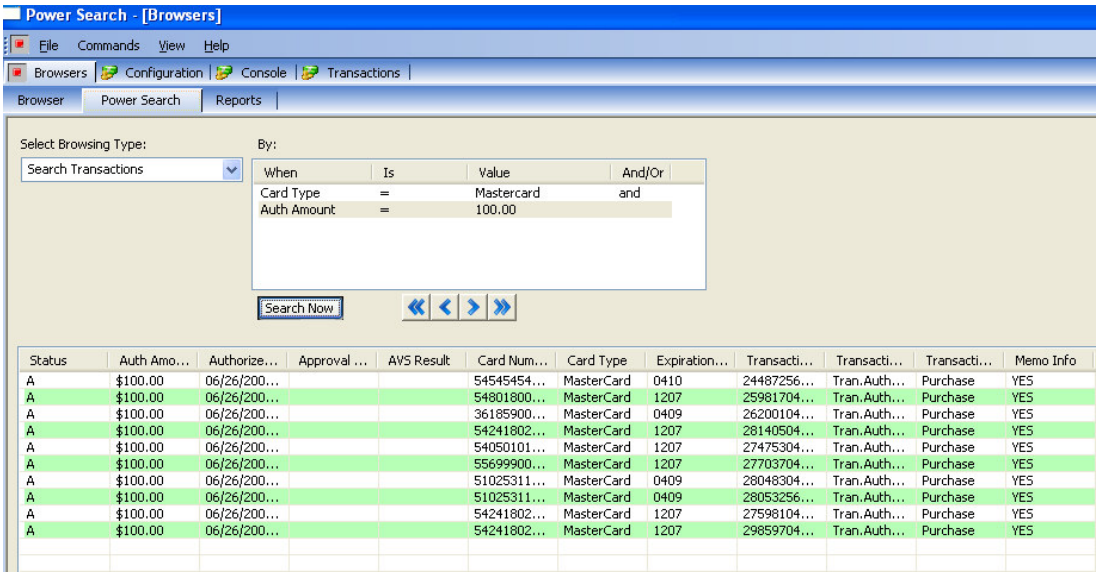
Occasionally, batches may be completed with an unknown status. Typical causes of this could be a communications error between TranScend™ and the processor, with this error occurring after the batch has been delivered to, and processed by, the processor. When these kinds of events occur, TranScend™ will mark the batch as being in an unknown status. When this occurs, you should contact your processor and/or TranScend™ customer support for more assistance. If the deposit was found to be successful, then you would select this command against the batch with the unknown status and mark it as being closed (successfully deposited).

Error Batch

Selection of this command will mark an unknown batch to an error state. See the discussion above for why batches may be placed into an unknown state.

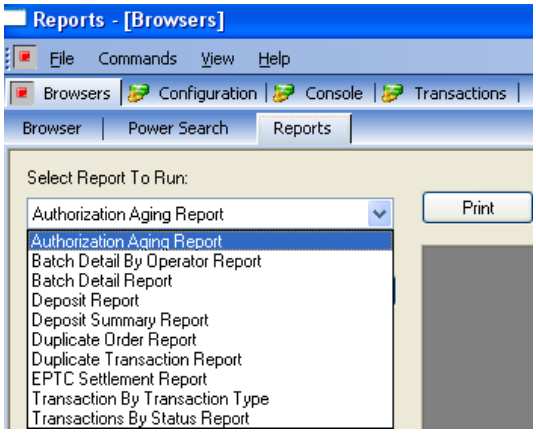
Power Search

This function allows the user to interact with a more precise record lookup tool. The user can define any number of specifics for the record(s) being sought and then can request the system to search for any records that match the specific criteria. For example: A user is looking to reconcile a transaction, but only has limited information, the purchase value ($100) and type of card (MasterCard). The user can utilize Power Search by selecting browsing type from drop-down box “Select Browsing Type” and right-clicking on the box entitled “By” and inserting the known information and selecting “Search Now”. If there are any transactions that meet the given criteria, they will appear on the screen provided.



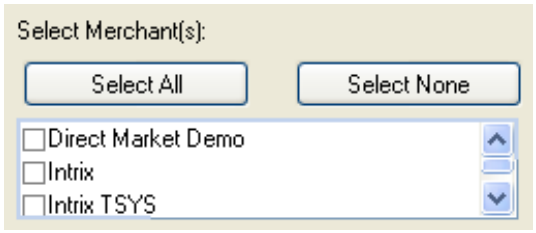
Running Reports

TranScend™ Reports can be displayed directly on the screen, printed, exported to PDF-files, HTML-files, RTF-files, XML-files or Excel spreadsheets. With this feature, users are able to select specific reports to view along with various merchants and transaction types. This is an essential element to the TranScend™ system allowing users to keep records of previous transactions. An explanation of each of the reporting-related controls will be provided below.



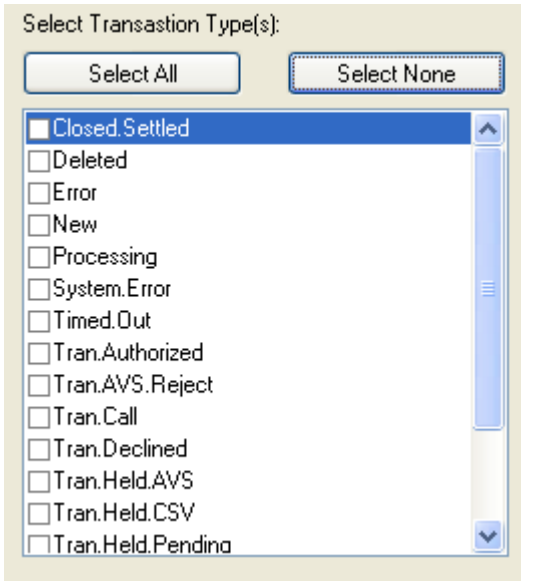
Select Report to Run

This is a list of various types of reports from your database. Items listed here will allow you to specify what type of report and what items to be viewed on the report created.



Merchant Selection

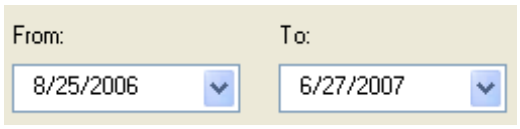
This allows the operator to determine which merchants to include in the results for a report.



Transaction Type

This is the list of transaction types to include in a report's results.

NOTE: List options vary depending on which report is selected to run.



Data Range

This option is used to define the range of dates to include in the results. The "From Date" defines the start date for the data records to be included in the report results. The "To Date" defines the end data for the data records to be included in the report results.

Load Report

Once all the report parameters are defined, then clicking this button issues a report command to the system. The resulting report data will be displayed in the space on the right hand side of the screen.

Authorization Aging Report

The Authorization Aging Report displays the authorizations that are waiting to be settled (for example: P = Purchase or A = Auth Only). The amount held against the cardholder's account will naturally expire in 7-12 days (occasionally some processors may have a different expiration period). Authorizations that expire (e.g., when an item is on back order) will need a new Authorization submitted.

Batch Detail by Operator Report

The Batch Detail by Operator Report allows you to view details of transactions created by each Operator. This may be used to keep track of the workload and efficiency of each individual operator (e.g., provide commission for operators). Below is a sample report to show an example of the information.

Batch Detail Reports

The Batch Detail Reports allow you to view details of batches between the dates ranges specified. This may be used to keep track of the amount of transactions completed during settlement. You can view total payments received as well as credits given. Below is a sample report to show an example of the information you will see.

Deposit Record Report

The Deposit Record Report allows you to print a report based on total amount by Merchant, transaction type, and date. This report will also show you a breakdown of dollars settled by card type and transaction.

Deposit Summary Report

The Deposit Summary report will display a report based on merchant selection and date preferences.

Duplicate Orders Report

Occasionally duplicate orders may be entered. The Duplicate Orders Report allows you to view the duplicate order numbers between the date range specified within the Reports screen in TranScend™ The Duplicate Order Report will select transactions where the Order Number is the same.

Duplicate Transaction Report

Occasionally duplicate transactions may be entered. The Duplicate Transaction Report allows you to view the duplicate transactions between the dates specified within the Reports screen. The Duplicate Transactions Report will select transactions where the credit card number, amount and transaction type are the same.

Transaction By Transaction Type Report

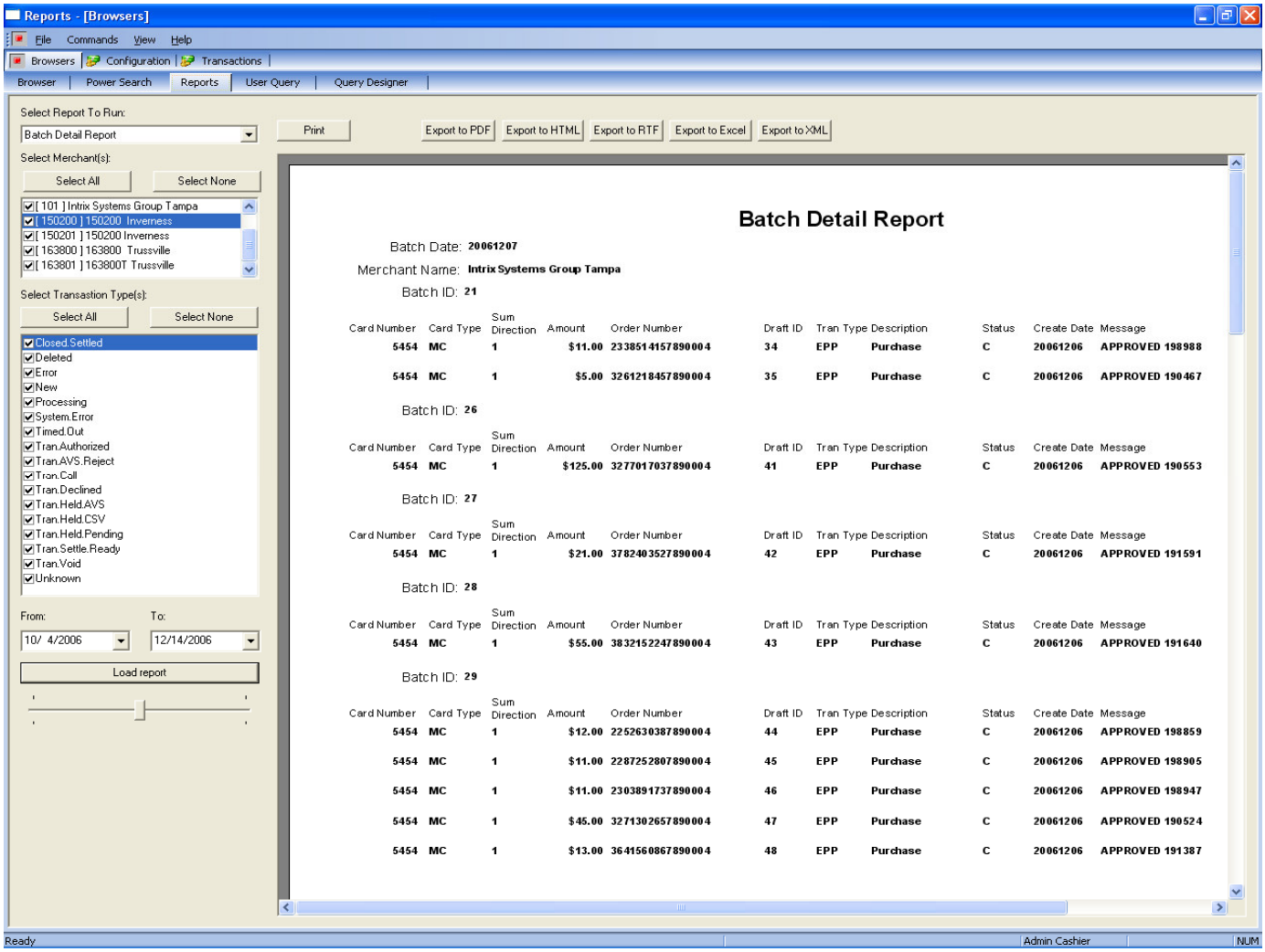
The Transaction By Transaction Type Report will display based on what is specified in the set up, the report will show subtotals for each merchant.

Transaction Subtotal By Status Report

The Transaction Subtotal By Status Report will display the status of transactions in your database between the date ranges specified within the Reports screen in TranScend™.

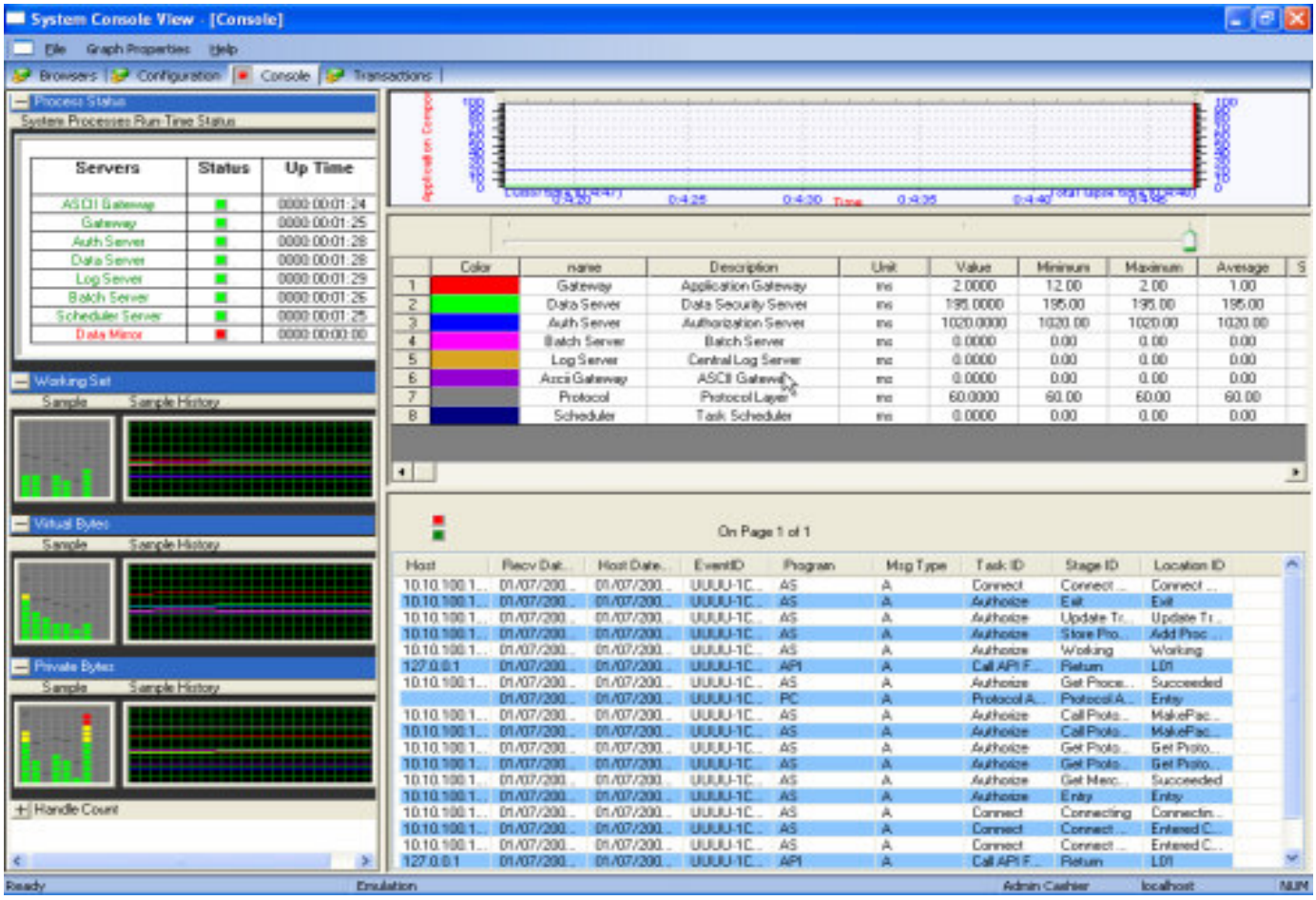
Sample Report Display

The image shown immediately below shows what the report display window looks like when a report has completed execution with the given parameters.



System Console

The System Console offers the most comprehensive view into the operations of TranScend™. The System Console connects to the Log Server as an "observer of the log stream" which means that each message received in the log will be "echoed" to the System Console. This allows the System Console to have a "real time view" into the operation of the system as it is running. As each command message is processed, the Gateway Server will generate a "command-processing timing-record" for that transaction. The timing-record shows the total processing time for that request, and as complete a break down as possible of the message processing time for each system component that was involved in processing that command. Finally, the System Console interacts with the Control Server to get a view of the "up time status" thus providing the system administrator with a way to observe the state of all the system components that compose the TranScend™ Processing Architecture (TPA).

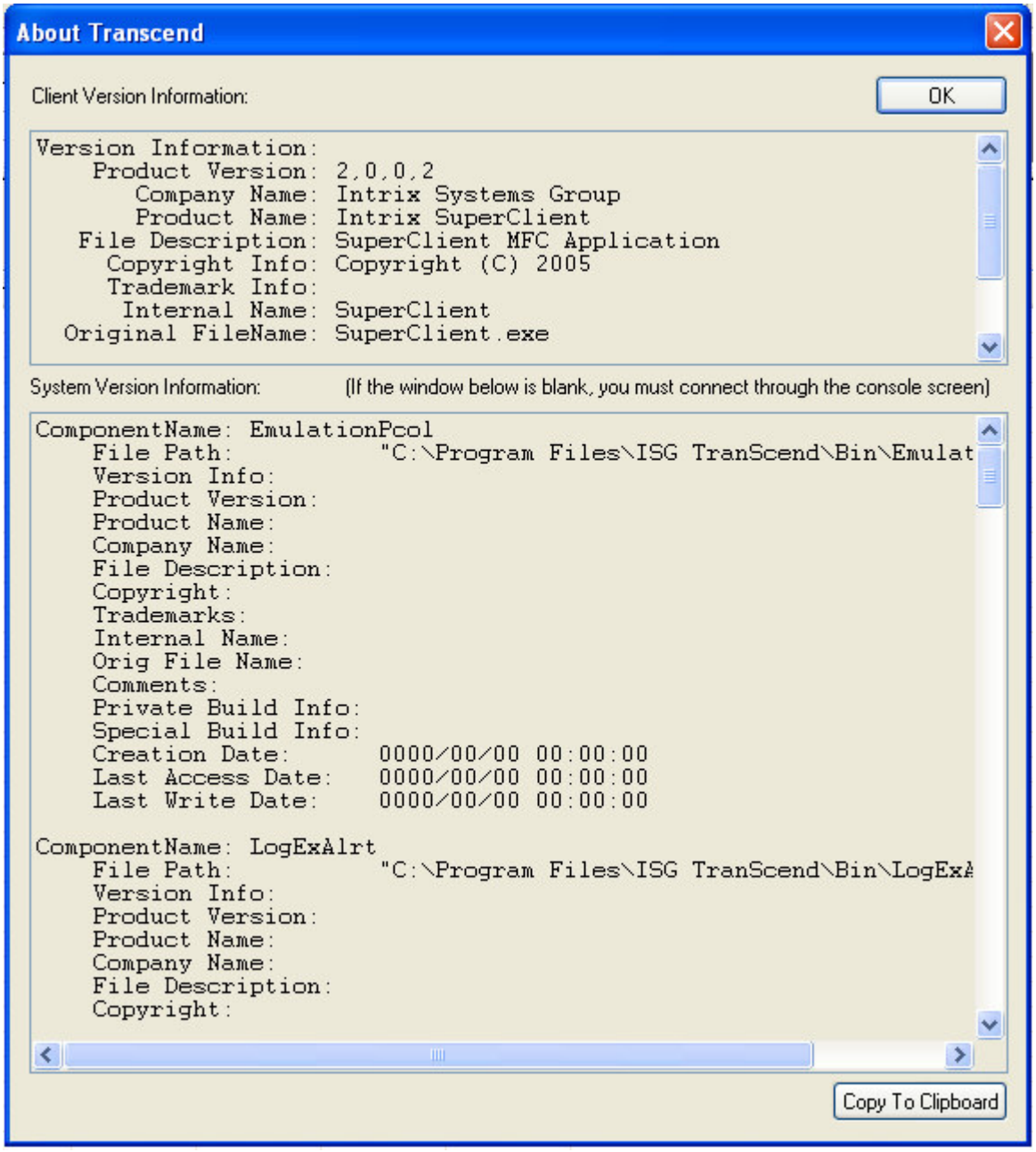


Connecting to TranScend™

- Click "File" from top level command menu
- Click "Connect" from drop-down menu. This connection allows the console to completely communicate with all components of TranScend™.

System Component Versions

With the Console View being active, the user can discover version information about the server-side components of the TranScend™ installation. To locate version information, click “Help” from the top level command menu. With Console connected, the “About TranScend™” can provide critical system information that you may be required to send INTRIX Support. In the event that you are asked to provide this information to support, use the “Copy To Clipboard” option and then paste this information into an email.



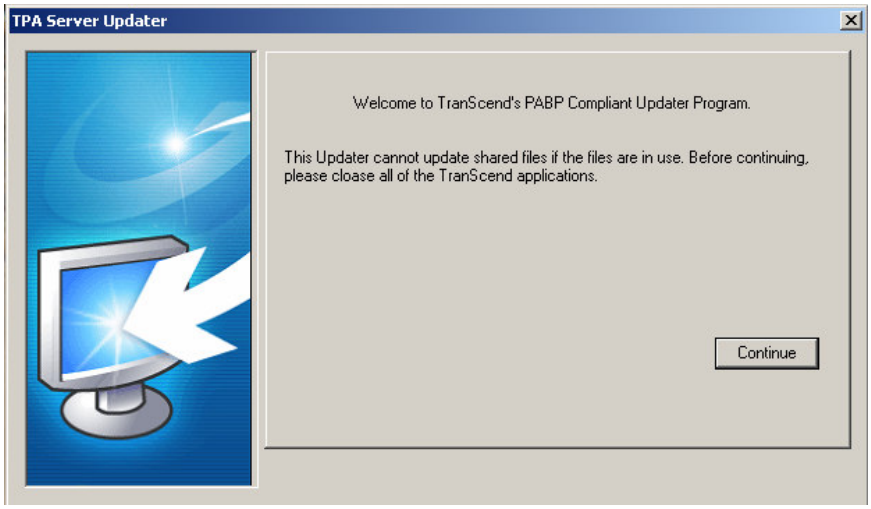
The image above shows a typical dialog that will be displayed when the “About TranScend™” menu command is initiated, with the option of “Copy To Clipboard”

System Updates

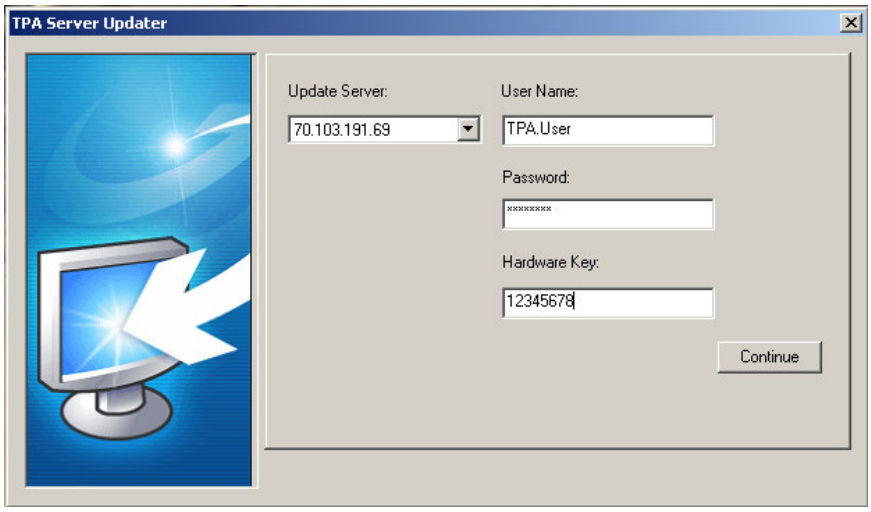
TranScend™ utilizes a customized system update process that was designed to meet the very specific industry requirements of the transaction processing industry with specific attention paid to PABP (Payment Application Best Practices) requirements. In addition, the system update process is also designed to provide additional security to users of TranScend™ through the following features:

1) The Addresses for the Update Servers are built into the system to reduce the possibility that malicious code can come from any other non-authorized source.
2) The communications protocol between the update client and the update server leverages SSL and standard HTTPS ports, but utilizes a proprietary data exchange protocol that no other non-authorized servers can easily replicate. This combined with #1) above provide the utmost security with regards to the source for any system updates.
3) Access to Updates is password protected with a "three way credential" that utilizes unique usernames and passwords. In addition, these credentials are also associated with the system's license key so as to protect the merchant's identity with an additional authentication factor.
4) Access to Server and Client Updates can be segregated among users within a merchant profile with Intrix. For example, consider that you'd like Fred to be able to update clients at your location, but not have the ability to update servers. Also, you'd like Gary to be able to update both servers and clients at your location, when these "download accounts" are set up on the Intrix Update Servers, you can specify which users are allowed to update which components of the system.
5) The Update program is transactional by design. It will either completely apply an update, or the entire update job will be "rolled back" completely and not applied to the target machine at all. This feature is incorporated to reduce the chances that a "partial update" is applied on the system.
6) The Update program is designed to preserve all files to the maximum extent possible. Files that are about to be overwritten are copied into back up directories whenever possible.

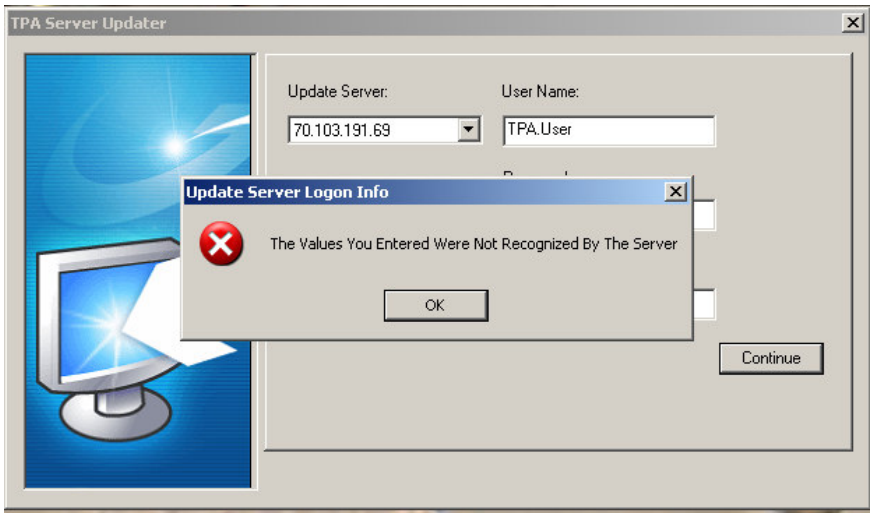
In the screen shots that follow, the server update process is examined in detail. The server update process and the client update process operate in near identical fashion except that they are specifically built to manage only one type of update (client update or server update). Any screen shot that is specific to only a single type of update will be pointed out as such.



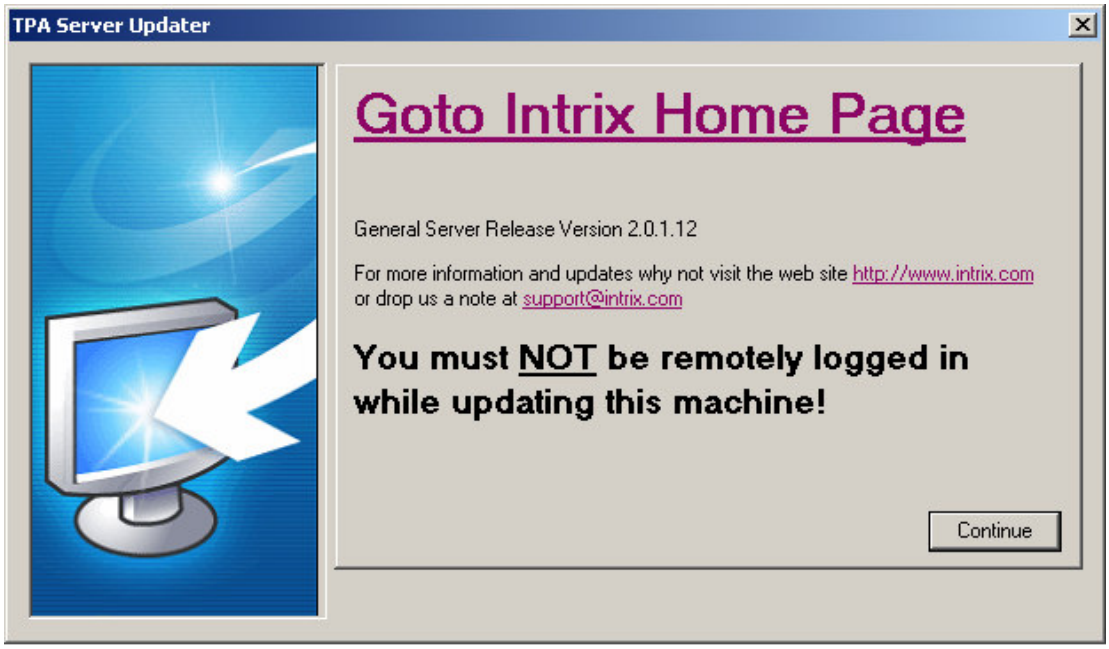
The first screen that will be seen is a typical "Welcome Screen." This screen is common to both versions of the installer.



After clicking "Continue" on the welcome screen, the screen shown above will appear. This screen allows you to select from a list of servers where updates will be placed by Intrix personnel. The User-Name, Password, and Hardware Key values will be assigned to you by Intrix when you purchase a license for the product.

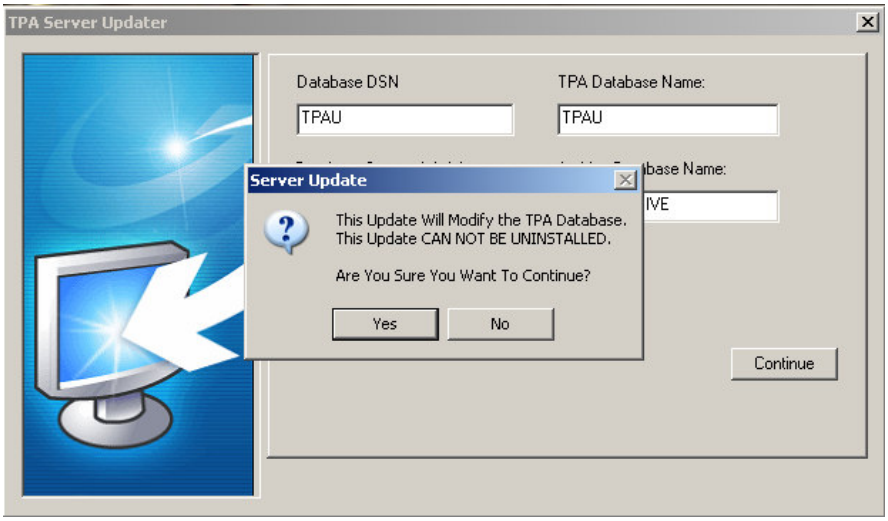


If the credentials you entered into the logon screen were incorrect, then you would be shown a message box indicating that the information provided was not accepted.

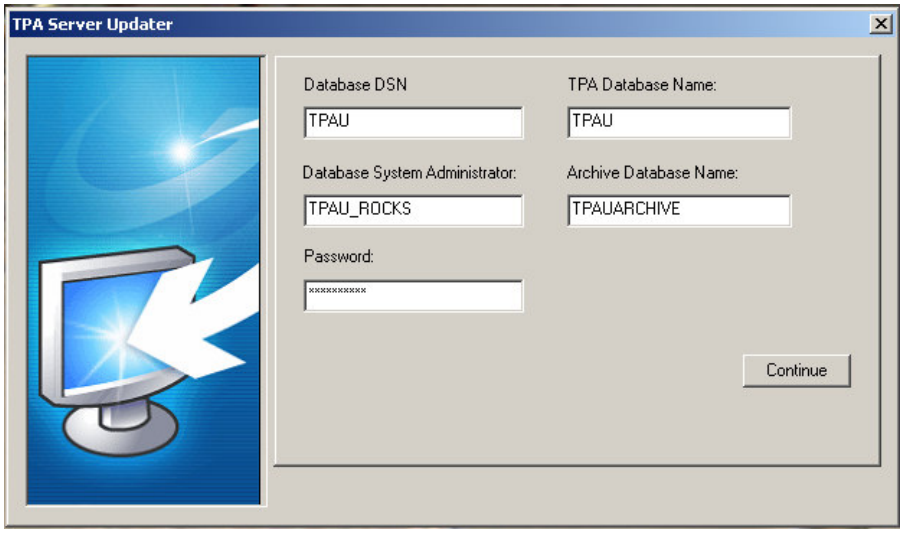


If the user credentials you supplied to the update server were accepted, then you may be shown an information screen like the one shown directly above. However, it is worth noting that this screen may vary for each update placed on the update servers. So, in some cases the appearance of this screen will be very different than the example shown above. In other cases, the screen may not be shown at all.

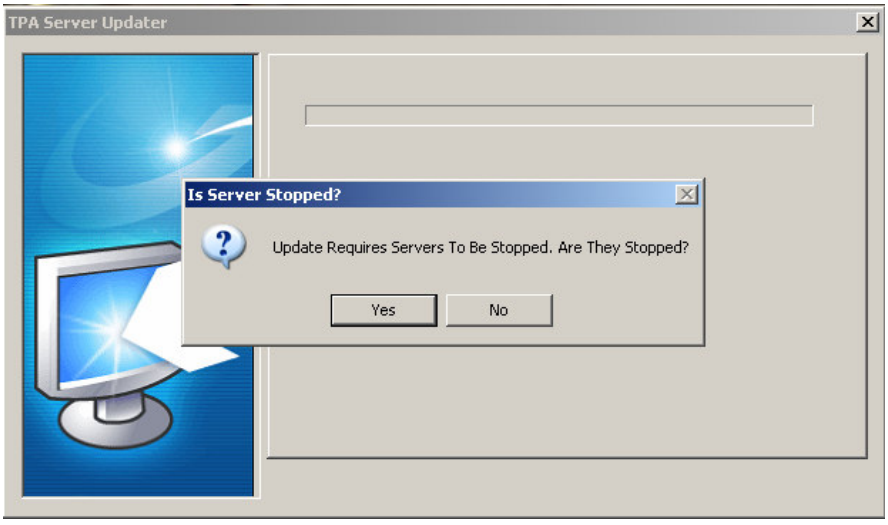
Note: In all cases the update should not be run remotely.



If the server update job requires a database change then you will be shown a message box alerting you to the fact that the database will be modified. If you click the “No” button on this message box, the update will quit and the program will exit. If you click “Yes” to this message box you will be dismissed and you see the underlying screen which is shown immediately below.

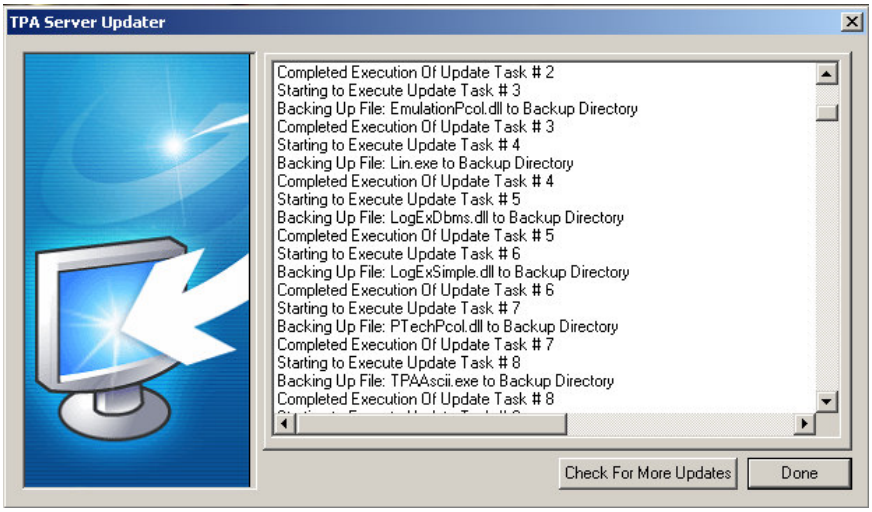


The screen shown immediately above will only be seen on server updates. This is because client updates are never expected to update the system database. You can also see that all the edits are pre-filled with working default values. However, if you have created a customized installation at your location, then you may have to change some of these values. It is important that these values be correct because if they are not the database updates may not work properly leaving your system in an inconsistent state. Prior to running a database update, a complete "user table snapshot" of all TranScend™ tables will be stored in the system database. After the update is completed, another "table snapshot" will be performed. This is done in the event that these tables may have to be restored to their previous state as part of manually repairing a failed database update.

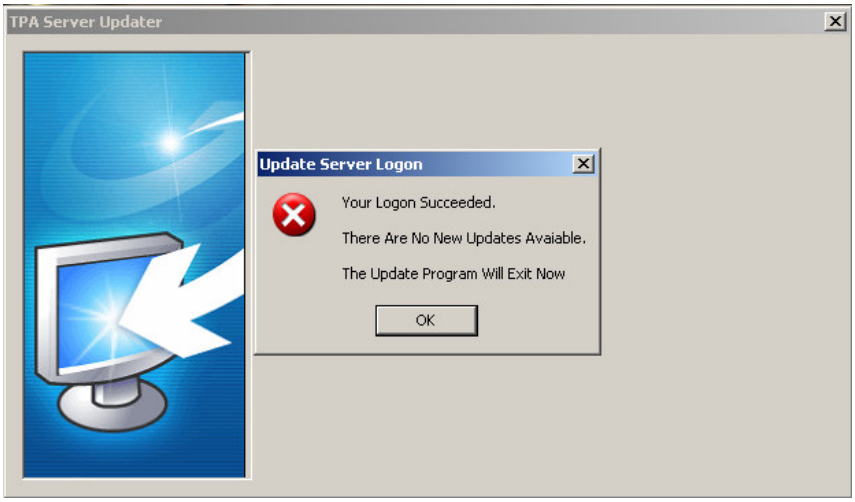


This is the last message you will be shown prior to the installation job being applied to your system. Since the system files may be replaced by the update, all the programs must be stopped. However, the only safe way to stop the system is for the user to do so. This being true, the user is asked to confirm that the system is stopped prior to starting the update. The update program will wait here indefinitely while the system is stopped. If you click "No" on this message box, then the update process will stop and no further actions will be performed. If you click "Yes" to this box, the update will immediately begin and you will activity in the progress bar (shown in the above image behind the message box). Once the progress bar reaches 100% the screen will change to the messages screen shown below. If there is an error during the update process, then

the progress bar will begin to “countdown” while the update is removed from the system and the system is restored to its prior state.



Once the update job is completed, you may choose to review the messages shown in the message list. The messages are also preserved in a log file that was created while the update job was being executed.



If you check for any newer updates with the update program, and no new updates have been loaded onto the Update Servers at Intrix, then you will see the message box shown immediately above and when that message box is dismissed the program will exit.

Appendix A: License Agreement and Warranty

License and Warranty

You must agree to the License Agreement before you can use TranScend™.

MASTER END-USER LICENSE AGREEMENT

IMPORTANT-READ CAREFULLY: This License Agreement is a legal agreement between you (either an individual or a single entity) and INTRIX Technology, Inc. (INTRIX) for the software product(s) accompanying this installation, which include(s) computer software and may include "online" or electronic documentation, associated media, and printed materials ("SOFTWARE PRODUCT").

By installing, copying, or otherwise using the SOFTWARE PRODUCT or any UPDATES (as defined below), you agree to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, do not install, copy, or use the SOFTWARE PRODUCT, and promptly return the entire unused SOFTWARE PRODUCT to your place of purchase for a full refund.

In addition, by installing, copying, or otherwise using subscription updates that you have received as part of the SOFTWARE PRODUCT ("UPDATES"), you agree to be bound by the additional license terms that accompany such UPDATES. If you do not agree to the additional license terms that accompany such UPDATES, you may not install, copy, or use such UPDATES.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed through INTRIX, not sold. The SOFTWARE PRODUCT consists of product documentation, sample applications, books, miscellaneous technical information, operating systems, applications, and other miscellaneous tools (individually identified as “COMPONENT" and collectively as "COMPONENTS"). The COMPONENTS contained in the SOFTWARE PRODUCT are determined by the product(s) you have elected to receive. The rights regarding the COMPONENTS of the SOFTWARE PRODUCT are described below unless otherwise indicated.

1. APPLICABILITY OF LICENSE

This agreement is applicable to licensees of the SOFTWARE PRODUCT through INTRIX. Depending on the product(s) you have elected to receive, the SOFTWARE PRODUCT may include any one or more of the following components: Samples, Programs, Documentation, and Tools.

2. GRANT OF LICENSE

To the extent that you have elected to receive a SOFTWARE PRODUCT from INTRIX, INTRIX grants to you as an individual a personal, nonexclusive license to make and use copies of the SOFTWARE PRODUCT in the manner provided below. If you are an entity, INTRIX grants to you the right to designate one individual within your organization to have the right to use the SOFTWARE PRODUCT in the manner provided below.

INTRIX grants to you, as an individual, a personal, nonexclusive license to make and use copies of the software portion of the SOFTWARE PRODUCT for the sole purposes of using the products only for the tasks for which it was designed for. You may install copies of the SOFTWARE PRODUCT on up to ten (10) computers, provided that you are the only individual using the SOFTWARE PRODUCT.

In addition, INTRIX grants to you, as an individual, a personal, nonexclusive license to make and use an unlimited number of copies of any documentary material from the documentation portion of the SOFTWARE PRODUCT ("Documentation"), provided that such copies shall be used only for personal purposes and are not to be republished or distributed (either in hard copy or electronic form) beyond the user's premises and with the following exception: you may use the Documentation identified with the product(s) solely in connection with your use of the software, provided, however, that the Documentation shall not be used in the development of a competitive application.

3. ADDITIONAL COMPONENT LICENSING TERMS

Each COMPONENT may have its own license agreement included with such COMPONENT ("Component Agreement"). In the event of inconsistencies between this agreement and any Component Agreement, the terms of the Component Agreement shall control except for the following:

(a) For all of the SOFTWARE PRODUCT, Section 4.1 of this agreement shall control;

(b) For all UPDATES and COMPONENTS received through the any distribution or resale channel, Section 10 of this agreement shall control; and

(c) For all COMPONENTS included in this distribution, all of the provisions of this agreement shall control.

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

4.1 ALL OF THE SOFTWARE PRODUCT

LIMITATIONS ON REVERSE ENGINEERING, DECOMPILATION, AND DISASSEMBLY. You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law, notwithstanding this limitation.

SEPERATION OF COMPONENTS. The SOFTWARE PRODUCT is licensed as a single product. Its COMPONENT parts may not be separated for use by more than one user (or for use on more than one computer for server software).

PRODUCT USE. The SOFTWARE PRODUCT may only be used for development purposes as described in Section 2 and may not be used in a production environment, unless such use is allowed under the terms of the Component Agreement delivered with the respective COMPONENT.

SUPPORT SERVICES. INTRIX may provide you with support services related to the SOFTWARE PRODUCT ("Support Services"). Use of Support Services is governed by the INTRIX policies and programs described in the user manual, "online" documentation, and/or INTRIX-provided materials. Any supplemental software code provided to you as part of the Support Services shall be considered part of the SOFTWARE PRODUCT and subject to the terms and conditions of this agreement.

With respect to technical information you provide to INTRIX as part of the Support Services, INTRIX may use such information for its business purposes, including for product support and development. INTRIX will not utilize such technical information in a form that personally identifies you.

TERMINATION. Without prejudice to any other rights, INTRIX may terminate this agreement if you fail to comply with the terms and conditions of this agreement. In such event, you must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

4.2 RESTRICTED USE OF SOFTWARE PRODUCT

With respect to the SOFTWARE PRODUCT, COMPONENTS of the SOFTWARE PRODUCT, each copy of such COMPONENT may be used by no more than two (2) processors of each computer on which such copy is installed. You may use the SOFTWARE PRODUCT as interactive workstation software on each computer on which the SOFTWARE PRODUCT is installed (a "Workstation Computer"), but not as server

software. However, you may permit a maximum of computers as referenced in the license key purchased to connect to the Workstation Computer to access and use services of the SOFTWARE PRODUCT. The connection maximum includes any indirect connections made through software or hardware that pools or aggregates connections.

(a) NO COMMERCIAL USE. You may not use the Software as part of or as the basis for a commercial public access data network that consists of two or more servers and that carries end-to-end electronic information traffic, such as messaging, data replication, fax, EDI, or telex, unless you obtain a separate commercial-use license from INTRIX.

(b) VERSION LIMITATION. The Server Software contains a certain version number (such as version "3.5"). This License permits you to install: (i) one (1) copy of the Server Software, (ii) with the same (or a lower) version number as the Server Software version number listed above, (iii) on a single computer (for example, if the version number listed above is "3.5," you may install Server Software that contains a "3.5" or "2.0" version number, but not a "3.6" version number).

The Distribution media on which SOFTWARE PRODUCT resides may contain a copy of other products produced by INTRIX. Note that in order to install or use this software, you must acquire a separate license for these products. You may not disclose the results of any benchmark test of either the Software to any third party without INTRIX's prior written approval.

Note Regarding the Use of Run-Time Software.

INTRIX hereby grants to you a limited, nonexclusive, royalty-free right to reproduce and distribute those files required for run-time execution of compiled applications ("Run-Time Files") in conjunction with and as a part of your application software product that is created using the INTRIX SOFTWARE PRODUCT, provided that: (a) you do not use INTRIX's name, logo, or trademarks to market your software product; (b) you include a valid copyright notice in your software product; (c) if your software product contains any redistributable files, it must include a valid copyright notice and you must distribute all components specified in the Readme file in conjunction with your software product; (d) you do not charge separately for the Run-Time Files; (e) you do not modify the Run-Time Files; and (f)you agree to indemnify, hold harmless, and defend INTRIX and its suppliers from and against any claims or lawsuits, including attorney's fees, that arise or result from the use or distribution of your application software product.

5. PRERELEASE CODE

Portions of the SOFTWARE PRODUCT may be identified as prerelease code ("Prerelease Code"). Such Prerelease Code is not at the level of performance and compatibility of the final, generally available product offering. The Prerelease Code may not operate correctly and may be substantially modified prior to first commercial shipment. INTRIX is not obligated to make this or any later version of the Prerelease Code commercially available. The grant of license to use Prerelease Code expires upon availability of a commercial release of the Prerelease Code from INTRIX.

6. SAMPLE CODE

INTRIX grants to you a nonexclusive, royalty-free right to use and modify the source code version of, and to reproduce and distribute the object code version of the Sample Code, provided that you comply with Section 8.

7. REDISTRIBUTABLE CODE

INTRIX grants to you a nonexclusive, royalty-free right to reproduce and distribute the DLL files included as part of the Sample Code, and additional rights to the SOFTWARE PRODUCT designated as "Redistributable Code," provided that you comply with Section 8.

8. DISTRIBUTION REQUIREMENTS

If you are authorized to redistribute the Redistributable Code (collectively "REDISTRIBUTABLE COMPONENTS") as described in Sections 6 and 7 above, you must (a) distribute the REDISTRIBUTABLE COMPONENTS only in conjunction with and as a part of your software product that adds primary and significant functionality to the REDISTRIBUTABLE COMPONENTS; (b) not permit further redistribution of the REDISTRIBUTABLE

COMPONENTS by your end-user customers; (c) not use INTRIX's name, logo, or trademarks to market your software application product; (d) include a valid copyright notice on your software product; (e) agree to indemnify, hold harmless, and defend INTRIX from and against any claims or lawsuits, including attorney's fees, that arise or result from the use or distribution of your software product; (f) otherwise comply with the terms of this license agreement; and (g) agree that INTRIX reserves all rights not expressly granted. Notwithstanding subsection 8(b), above, you may permit further redistribution of the REDISTRIBUTABLE

COMPONENTS by your distributors to your end-user customers if your distributors only distribute the REDISTRIBUTABLE COMPONENTS in conjunction with, and as part of, your Application and you and your distributors comply with all other terms of this agreement.

9. COPYRIGHT

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets," incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by INTRIX or its suppliers. The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may either (a) make one copy of the SOFTWARE PRODUCT solely for backup or archival purposes, or (b) install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the SOFTWARE RODUCT.

10. UPDATE LICENSE TERMS

Additional license terms may accompany UPDATES (as defined in the first paragraph of this agreement). By installing, copying, or otherwise using any UPDATE, you agree to be bound by the terms accompanying each such UPDATE. If you do not agree to the additional license terms accompanying such UPDATES, do not install, copy, or otherwise use such UPDATES.

11. SUBSCRIPTION UPDATES

You may use or transfer the UPDATES only in conjunction with your then-existing SOFTWARE PRODUCT. The SOFTWARE PRODUCT and all UPDATES are licensed as a single product and the UPDATES may not be separated from the SOFTWARE PRODUCT for use by more than one user at any time.

12. EXPORT RESTRICTIONS

You agree that neither you nor your customers intend to or will, directly or indirectly, export or transmit the SOFTWARE PRODUCT or related documentation and technical data (or any part thereof), or your software application product as described above (or any part thereof), process, or service that is the direct product of the SOFTWARE PRODUCT to any country to which such export or transmission is restricted by any applicable U.S. regulation or statute, without the prior written consent, if required, of the Bureau of Export Administration of the U.S. Department of Commerce, or such other governmental entity as may have jurisdiction over such export or transmission.

13. U.S. GOVERNMENT RESTRICTED RIGHTS

The SOFTWARE PRODUCT and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer

Software-Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is INTRIX Technology, Inc. at 2260 Douglas Blvd., Suite 240, Roseville, CA 95661, (916) 577-1315.

DISCLAIMER OF WARRANTY NO WARRANTIES

The software product is provided “as is” without warranty of any kind. To the maximum extent permitted by applicable law, INTIRX Technology, Inc. and its suppliers disclaim all warranties, either express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose and any warranty against infringement, with regard to the software product. This limited warranty gives you specific legal rights. You may have others, which vary from State/Jurisdiction to State/Jurisdiction

CUSTOMER REMEDIES

INTRIX Technology, Inc.’s entire liability and your exclusive remedy shall not exceed the price paid for the software product.

NO LIABILITY FOR DAMAGES

To the maximum extent permitted by applicable law, in no event shall INTRIX Technology, Inc. or its suppliers be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use this INTRIX Technology, Inc. product, even if INTRIX Technology Inc. has been advised of the possibility of such damages. Because some States/Jurisdictions do not allow the exclusion or limitation or liability for consequential or incidental damages, the above limitation may not apply to you.

MISCELLANEOUS

If you acquired this product in the United States, this agreement is governed by the laws of the State of California.

If this product was acquired outside the United States, then local law may apply.

Should you have any questions concerning this agreement, or if you desire to contact INTRIX for any reason, please contact the INTRIX subsidiary serving your country, or write: INTRIX Technology, Inc. 2260 Douglas Blvd., Suite 240, Roseville, CA 95661.

Appendix B: TranScend Database Backup Strategy

Overview

The obvious goal of database backups is to ensure the safety and integrity of the data held in the database. The less obvious goal is to minimize the time taken to restore the database in the event of a failure while also keeping the costs of backing up the database reasonable. Costs, in this context, are the demands placed on the database engine related to database backup operations.

Database Backup Tools At Your Disposal

MS SQL Server offers 3 different kinds of backups, which are:

1. Full Database Backup
2. Differential Backups (wherein all the differences from the last full backup are backed up)
3. Transaction Log Backups (backs up the database transactions since the last full, differential or transaction log backup)

Now, to restore a database, a typical approach that utilizes SQL Server's these tools would be as follows:

1. Restore last full backup
2. Restore differential backups that were made subsequent to the last full backup
3. Restore transaction log backups that were made subsequent to the last differential backup

However, restoration of transaction log backups is a very expensive operation, and consumes a significant amount of system resources. Therefore, TranScend™'s Development Team has devised additional strategies that are designed to create more rapid database restoration after a fault has occurred that requires a database restoration.

NOTE: All customers are advised and encouraged to real about all topics related to BACKUP and RESTORATION in SQL Server Books Online. To find the current location of this very important resource do the following:

- Perform an internet search for the topic: "SQL Server Books Online" and "BACKUP"
- Navigate to the appropriate location on the Microsoft Site
- Read and try to understand the information provided in terms of your business' needs for data backup and restoration techniques

Making use of TranScend Features to Assist Database Restorations

The TranScend™ system keeps a complete "delta log" of all the records written to the system. The TranScend™ delta-record log is a set of text files that contain each SQL statement that is applied to the TranScend™ database. This data format can be "directly played into" a SQL Server database, which allows the user of TranScend™ an improved restoration approach beyond what SQL Server tools by themselves can provide. Because of this, customers will restore databases in the following sequence:

1. Restore last full backup
2. If using any Full or Differential Restoration Motel, then next you should restore the most recent differential backup made subsequent to the last full backup
3. Restore TranScend™'s Delta logs that were made subsequent to the last differential backup

NOTE: There is no security risk for the data records in the TranScend™ delta log file, as all data of a potentially sensitive nature is encrypted prior to being written to the delta record log file.

Backup of the TranScend Databases

There is no practical way for TranScend™ to perform automated backups of your database. This is because each business has its own operational hours and because backing up databases must occur in within your system's maintenance window. With this in mind, each customer must take a role in backing up the databases on a regular basis using the following schedules as a recommended starting point.

- Full Backup should be performed at least once a week
- If using a Full or Differential Model, then Differential Backups and Transaction Log backups should be performed daily.

Based on the back up strategy in place at your organization, the following operations would be needed to restore the database data-image after a database crash or data corruption, the customer will have to:

1. Restore the last full backup
2. If using a Full or Differential Model, the next step is to restore the most recent differential backup
3. Replay all TranScend™ Delta-Record Files containing data that were made after the most recent differential backup.

Note that the nature of the SQL contained in the Delta Record Logs is designed to make the best use of the referential integrity built into the TranScend™ database. Therefore, these SQL statements are formatted such that there is no harm done by replaying Delta Record Log data that is "earlier occurring" than the last differential backup, as those changes (as appear in the delta record log) will simply "bounce off" the database.

However, it is very important that ALL delta record log files made subsequent to the last differential backup be applied during the restoration process, so that the database image is restored to the "maximum extent possible" and to mitigate to the highest degree possible the possibility of any data loss.

After any database restoration has become required, the data within the database should be "inspected" to the greatest degree possible to verify that there is in fact no data lost. While the TranScend™ system is designed to eliminate these threats to the greatest degree possible, there are many factors and failure modes that are simply beyond the control of TranScend™ and therefore can not be fully accounted for.

Customer Responsibility

The customer must recognize and accept responsibility for the "health and safety" of the TranScend data for the following reasons:

1. It is important for the customer to recognize that the data created by TranScend is data that belongs to your organization, and since it is financial in nature it should be an important priority to your organization to monitor the health and safety of the database and the data contained therein. Should an unrecognized fault occur due to lack of attention to the database itself, you must remember that it is primarily your business that will be affected by any subsequent data loss that may occur.
2. While the TranScend™ Development team took database safety and restoration into account during their design and implementation, it is still true that the system runs at the customer's site, and because of this, the **CUSTOMER BECOMES THEIR OWN FIRST LINE OF DEFENSE** so far as monitoring the actual state of the database.

As database backup processes are run, they can produce output reflecting the success of the database backup operations. It is up to the customer to **review these logs on a daily basis to verify that there are no errors reported** during these operations. **ANY REPORTED ERROR** in these log files should be treated as **potential threat** to your company's data and should be **understood and corrected as soon as possible**.

It is also important to note that any errors that are reported during back up and restoration activities are errors reported by SQL Server engine. While Intrix Technology, Inc. can attempt to help with the identification of any problems reported by the DBMS, it is important to understand that Intrix Technology, Inc. can not directly address or repair any of these issues directly.

It is also important to understand that any maintenance agreement your company may have with Intrix Technology, Inc. **DOES NOT INCLUDE THE REPAIR** of database files caused by any faults encountered within the database engine. Because of this limitation, the customer is expected to have any appropriate support agreements in place with the DBMS vendor as the manufacturer of the DBMS is best equipped to address any issues affecting the database engine itself.

Appendix C: Credit Card Validation Rules

Mod-10 Verification

Most credit card numbers are encoded at the right end with a "check digit", there is a simple algorithm called "Luhn" or "Mod 10", which can verify that a credit card number has been entered correctly. To pass Mod-10, check the sum of the digits divided by 10 must yield an integer (whole number). Any value that is evenly divisible by 10 will be considered a successful credit card number entry. The "check digit" allows the card issuer to guarantee that the algorithm result (X) will be evenly divisible by 10.

For example, in the sample below when the calculated value (without the check digit) is 71, we know that the "check digit" number must be 9. The sum would equal 80, which is evenly divisible by 10. Using the card number 4444555566667779 as an example, here's how to calculate the result (X) in the X Mod-10 formula:

Reading from right to left (←), multiply the even positioned values by 2, and the odd positioned values by 1.

The following table demonstrates the first step (↓):

16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1◄
4	4	4	4	5	5	5	5	6	6	6	6	7	7	7	9 ▼
X2	X1	X2	X1	X2	X1	X2	X1	X2	X1	X2	X1	X2	X1	X2	X1
8	4	8	4	10	5	10	5	12	6	12	6	14	7	14	9

Now, add each "single" digit together to get the result (X). The following demonstrates this step:

8 + 4 + 8 + 4 + 1 + 0 + 5 + 1 + 0 + 5 + 1 + 2 + 6 + 1 + 2 + 6 + 1 + 4 + 7 + 1 + 4 + 9=80

Last, Perform Mod 10 on the Sum (X Mod-10 = 0):

80 mod 10 = 0, verified as correct

Credit Card Ranges

The credit card number length should be 13-16 digits. Also, individual card types use different opening digits:

Credit Card Type	Length	Range (Starts with)
American Express	15	340000-349999 370000-379999
Diners Club	14,16	300000-305999

		360000-369999 380000-389999
Discover	16	601100-601199
JCB	16	352800-358999
MasterCard	16	510000-559999
Visa	13,16	400000-499999

Appendix D: Testing Environment Settings

Emulation Mode

Emulation Mode Test Card Numbers

Credit Card Type	Credit Card Number
MasterCard	5424 1802 7979 1765
Visa	4005 5500 0000 0019
American Express	3732 3538 7881 007
Discover	6011 0009 9304 3615

Emulation Mode AVS Responses

These responses originate from within TranScend™ only in Emulation Mode

Address	***Zip***	***Result Codes***
any	11111	A -- 5 Zip Match
any	22222	E – Illegible
any	33333	"N -- No Match"
any	44444	"R -- System unavailable"
any	55555	U -- Address Info not Available
any	66666	Y – Zip Match, Plus 4
any	77777	Z – Zip Match, Plus 4
any	88888	G -- Issuer does not participate in AVS

Emulation Mode CVV2 Responses

These responses originate from within TranScend™ only in Emulation Mode

CVV2	***Result Codes***
111	M -- CVV2 Match
222	N -- CVV2 No Match
333	P -- Not Processed
444	S -- Merchant has indicated that Verification Code is not present on card
555	U -- Issuer is not certified or has not provided Visa encryption keys

Emulation Mode Auto Responses for Credit Cards

These responses originate from within TranScend™ only in Emulation Mode

Amount	Response Code	Response Text	Status
$ 0.01	01	Card declined	D
$ 0.02	02	Card declined	D
$ 0.03	28	No reply	D
$ 0.04	91	No reply	D
$ 0.05	04	Hold-Call	H
$ 0.06	07	Hold-Call	H
$ 0.07	41	Hold-Call	H
$ 0.08	43	Hold-Call	H
$ 0.09	EA	Verification Error	E
$ 0.10	79	Already Reversed at Switch	E
$ 0.11	13	Invalid amount	E
$ 0.14	14	Card Number Error	E
$ 0.15	82	CVV data is not correct	E
$ 0.16	N3	Cash back service not available	E
$ 0.17	EB	Verification Error (Check Digit Err)	E
$ 0.18	EC	Verification Error (CID Format Error)	E
$ 0.19	80	Invalid date	E
$ 0.27	81	Cryptographic error	E
$ 0.28	06	General error	E
$ 0.29	54	Expired card	E
$ 0.30	92	Destination not found	E
$ 0.31	12	Invalid transaction	E
$ 0.32	78	No account	E
$ 0.33	21	Unable to back out transaction	E
$ 0.34	76	Unable to locate, no match	E
$ 0.35	77	Inconsistent data	E
$ 0.37	39	No credit account	E
$ 0.39	15	No such issuer	E
$ 0.41	19	Re-enter transaction	E
$ 0.42	63	Security violation	E

$ 0.43	57	Transaction not permitted-Card	E
$ 0.44	58	Transaction not permitted-Terminal	E
$ 0.45	96	System malfunction	E
$ 0.46	03	Invalid Merchant ID	E
$ 0.48	N7	CVV2 Value supplied is invalid	E
$ 0.99	93	Violation cannot complete	E

Emulation Mode Auto Responses for Debit Cards

These responses originate from within TranScend™ only in Emulation Mode

Amount	Response Code	Response Text	Status
$ 0.01	01	Card declined	D
$ 0.02	02	Card declined	D
$ 0.03	28	No reply	D
$ 0.12	83	Cannot Verify PIN	D
$ 0.13	86	Cannot Verify PIN	D
$ 0.14	14	Card Number Error	E
$ 0.16	N3	Cash back service not available	E
$ 0.19	80	Invalid date	E
$ 0.29	54	Expired card	E
$ 0.36	52	No checking account	E
$ 0.38	53	No savings account	E
$ 0.40	75	PIN tries exceeded	E
$ 0.43	57	Transaction not permitted-Card	E
$ 0.45	96	System malfunction	E
$ 0.46	03	Invalid Merchant ID	E
$ 0.47	55	Incorrect PIN	E

Emulation Mode Auto Responses for Gift Cards

These responses originate from within TranScend™ only in Emulation Mode

Amount	Response Code	Response Text	Status
$ 0.01	01	Card declined	D
$ 0.02	02	Card declined	D
$ 0.03	28	No reply	D
$ 0.14	14	Card Number Error	E
$ 0.19	80	Invalid date	E
$ 0.29	54	Expired card	E
$ 0.43	57	Transaction not permitted-Card	E
$ 0.45	96	System malfunction	E
$ 0.46	03	Invalid Merchant ID	E

Appendix E: Security Best Practices

Overview and History

The following document is designed to give users of the TranScend™ application a better understanding of the recently implemented security policies in the payment processing industry. The document outlines the evolution of today's standards, describes the industry best practices for payment application and then instructs users of the TranScend™ application in areas not completely controlled by the payment application but necessary to implement the product in a CISP compliant manner.

Visa first introduced the Cardholder Information Security Program (CISP) in 2001. MasterCard was quick to follow suite with their security program called Site Data Protection Plan (SDP). Nearly six years later the industry has now evolved into a single standard endorsed by nearly every payment industry participant.

Visa's Cardholder Information Security Program (CISP)

CISP is the acronym for Visa's Cardholder Information Security Program, if you store, transmit, or process Visa cardholder data, then CISP does apply to you. By implementing CISP, Visa is placing the responsibility of protecting Visa cardholder data on everyone involved in the transaction process. As we all know, a chain is only as strong as its weakest link and it only takes one "open window" for cardholder data to be compromised.

How CISP Compliance Works

CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry.

CISP Compliance Validation Details

Separate and distinct from the mandate to comply with CISP requirements is the validation of compliance. It is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Visa has prioritized and defined levels of CISP compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the Visa system by merchants and service providers.

Acquirers are responsible for ensuring that all of their merchants comply with CISP, however, merchant compliance validation has been prioritized based on the volume of transactions, the potential risk, and exposure introduced into the Visa system.

Merchant Levels Defined

Acquirers are responsible for determining the compliance validation levels of their merchants. All merchants will fall into one of the four merchant levels based on annual Visa transaction volume. The transaction volume is based on the aggregate number of Visa transactions from a Doing Business As (DBA) or a chain of stores (not of a corporation that has several chains). Merchant levels are defined as:

Merchant Level	Description
1	Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. Any merchant identified by any other payment card brand as Level 1.
2	Any merchant processing 150,000 to 6,000,000 Visa e-commerce transactions per year.
3	Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6,000,000 Visa transactions per year.

CISP Compliance Validation Basics

In addition to adhering to the twelve security requirements and sub-requirements, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and strongly recommended for Level 4 merchants.

Level	Validation Action	Validated By
1	Annual On-Site Security Audit Quarterly Network Scan	Independent Security Assessor or Internal Audit if signed by Officer of the company Qualified Independent Scan Vendor

2 and 3	Annual Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor
4*	Annual Self-Assessment Questionnaire (Recommended) Network Scan (Recommended)	Merchant Qualified Independent Scan Vendor

*Level 4 merchants must comply with CISP; however, compliance validation for merchants in this category will be determined at the acquirer's discretion.

MasterCard's Site Data Protection Plan (SDP)

MasterCard's Site Data Protection Program (SDP). SDP provides a comprehensive approach to evaluating and improving web site security. The SDP Program provides acquiring members with the ability to deploy security compliance programs, ensuring that online merchants and Member Service Providers are adequately protected against hacker intrusions and account data compromises.

The SDP Program includes the following elements:

The MasterCard Security Standard*:* A series of manuals providing security requirements and best practices for participating acquiring members, online merchants, Member Service Providers, and data security vendors.

Evaluation Tools: Participants can demonstrate MasterCard Security Standard compliance by using the MasterCard Security Self-Assessment and Network Scanning Tools. With these tools, participants can self-evaluate their security situation and conduct real-time vulnerability assessments of their web infrastructure.

SDP Service: The MasterCard Site Data Protection Service is a proactive, cost-effective, global solution offered by MasterCard through its acquiring members. The SDP Service includes network vulnerability scans and alert services offered by our SDP Service partner, Ubizen.

Alternative Vendor Solutions: As an alternative to the SDP Service, participants may select any security vendor solution that is compliant with MasterCard Security Standard. If desired, acquirers can ensure vendor compliance through the use of an optional, fee-based vendor certification program offered by MasterCard.

Web Insurance: An optional discounted Marsh insurance policy, offers financial protection in case of a compromise.

Payment Card Industry Data Security Standard

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all card brands. This standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

PCI Data Security Standard Basic Requirements

The PCI Data Security Standard consists of twelve basic requirements supported by more detailed sub-requirements:

Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored data
- Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security

Payment Application Best Practice

The following has been taken directly from the Visa/CISP web site. Visa has developed *Payment Application Best Practices* to address security and the risks associated when full magnetic stripe data or CVV2 values are stored after authorization by payment applications. The best practices assist software vendors in creating secure payment applications that help ensure merchant CISP compliance.

Best Practices Goal

The goal of the Payment Application Best Practices is to help software vendors create secure payment applications. To be considered secure, these applications must not retain full magnetic stripe data or CVV2 data and must support a merchant's ability to comply with CISP requirements. Acquirers are responsible for ensuring that their merchants and service providers confirm the security of their payment applications using the *Payment Application Best Practices*.

Visa Recommendations

Visa has been actively working to educate software vendors and to provide best practices for secure payment applications where sensitive track data and CVV2 values are never stored subsequent to authorization. **Visa strongly recommends that:**

Software vendors validate their payment applications against recommendations outlined in Visa's *Payment Application Best Practices*. Visa makes no endorsement of applications or products and disclaims all warranties. Members remain responsible for performing their own evaluation and due diligence to ensure CISP compliance of their merchants and service providers.

Acquirers share the *Payment Application Best Practices* with both card-present and online merchants, and encourage them to use it to evaluate their current payment applications, as well as any pending payment application implementation. Acquirers and merchants can also encourage software vendors to participate in Visa's validation effort.

Acquirers refer to Visa's List of CISP-Validated Payment Applications and encourage their merchants to use CISP-validated payment applications.

Validation Procedures and Documentation

Software vendors seeking to validate their payment applications must engage a Visa-qualified independent security assessor to perform an on-site review and submit the required documentation to Visa. Compliance validation takes place at software vendor's expense, as follows:

The *Annual On-Site Security Audit* must be completed according to the *Payment Application Best Practices* document. This document is also to be used as the template for the Report on Validation. The scope of CISP validation is described in the *Payment Application Best Practices* download.

Assessors performing payment application reviews must contact Visa for approval before proceeding with the audit specified in the *Payment Application Best Practices*. Visa will not accept audits without this pre-approval.

Payment Application Best Practices Summary

The following are the high level best practices to follow in order to ensure the Payment Application complies with the *Payment Application Best Practices* document. Each high-level best practice has several additional elements that are tested during the certification process. The requirements for Payment Application Best Practices validation are derived from the Payment Card Industry (PCI) Data Security Standard and the PCI

Security Audit Procedures. These documents, detail what is required to be CISP compliant (and therefore what a payment application should do to facilitate a merchant's CISP compliance) and should be used as a reference for CISP standards. Validated applications must be capable of being implemented in a CISP-compliant manner.

1. Do not retain full magnetic stripe or CVV2 data.
2. Protect stored data.
3. Provide secure password features.
4. Log application activity.
5. Develop secure applications.
6. Protect wireless transmissions.
7. Test applications to address vulnerabilities.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to the Internet.
10. Facilitate secure remote software updates.
11. Facilitate secure remote access to the application.
12. Encrypt sensitive traffic over public networks.
13. Encrypt all non-console administrative access.

Client Implementation Documentation

In accordance with Visa regulations, software vendors are expected to provide product documentation to instruct their customers on secure product implementation. This documentation should clearly delineate vendor and customer responsibilities for meeting CISP requirements. It should detail the responsibilities of the customer to enable security settings within their own network, such as password security, which may not be controlled by the application but are required for CISP compliance.

The following instructions are designed to assist the users in areas not completely controlled by the payment application but necessary to implement the product in a CISP compliant manner.

Complex Passwords

How to create CISP Compliant Complex Passwords

When it comes to passwords you usually hear what you should **NOT** do:

• give your password to others

• choose short passwords

• use lowercase letters only

• use obvious passwords that are easy to guess

• reuse the same passwords

• write passwords down

Here are some sensible rules to follow for developing and remembering complex passwords:

Rule 1: Passwords should be at least 8 characters long and contain a combination of upper and lowercase characters, digits, and special characters like !,§ or #.

When a password is created, it is encrypted using a hash function and stored in this form. Later, a user is only granted access if the hash of the supplied password agrees with the stored value. Hash functions are constructed in such a way that they cannot be reversed. Instead, the attacker must use the brute force approach and try every single combination.

1. There are approximately 324 different passwords consisting of 6 lowercase letters. A cracker using L0phtCrack4 can test them all in less than 5 minutes.

2. There are approximately 6,090 different passwords consisting of 8 printable ASCII characters. It would take decades to try them all, even with today's computers.

Following Rule 1 should therefore foil brute force attacks, assuming the password system is implemented correctly.

Rule 2: Avoid passwords that can be guessed!

Some famous passwords are Joe. Joe accounts refer to accounts where the password is the same as the user name. President Clinton used the (well-known) name of his dog, Buddy, when electronically signing the electronic commerce bill. These are just as good as leaving the key under the mat. To avoid this, users were advised in the 90's to apply various sorts of transformations to their passwords, e.g. drowssap: password read backwards, pa$$word: substituting $ for s, etc.
Using transformations like the ones above, the worm dictionary introduced in 1998 could guess 50% of all passwords on the UNIX servers that it attacked. Today, there is a wide collection of these dictionaries available on the Internet. Since the guessing is done by programs these days, rule 2 implies that strong passwords should not contain any words or transformed words that can be found in a dictionary.

Rule 3: Good passwords are strong passwords that can be easily remembered.

We can quickly create a strong password like 1§kW8-qP&5 but we will soon forget it. A good strategy is to start with a phrase that you know well. Try using old songs that are not widely known. Taking the first character of each word produces a complex password that we can recreate without effort. Better yet, create your own unique phrases and take away letters or add special characters.

When to Use Complex Passwords

We strongly urge customers to assign strong application and system passwords whenever possible and the following best practices should be followed at all times:

- All applications should require a unique username and complex password for all administrative access and access to cardholder data.
- Access to PC's, servers and databases with payment applications should require a unique user name and complex password.

Manage Complex Passwords- Access To The Payment Application

Access to the TranScend™ Client should be granted to those individuals whose job function requires them to do so. A unique username should be assigned to each person accessing the utilities and only Active usernames with the proper password will be allowed into the system. All other access will be denied.

- Administrators who follow the best practice guidelines outlined in Payment Card Industry Data Security Standard dated January 2005 should educate the users and ensure policies according to the following:
- Immediately change the provided INTRIX Technology Inc., default password for System Administrator.
- Instruct users to create passwords a least 8 letters in length consisting of a combination of numeric, alphanumeric and special characters.
- Instruct users NOT to create a username and password that are the same.
- Implement a process whereby passwords to the TranScend™ Client are changed every 90 days but do not allow the new password to be the same as any of the user's previous 4 passwords.

CISP Compliant Log Settings

All TranScend™ log settings are CISP compliant. The logs are fully encrypted and log all access by individual users (especially those with administrative privileges), and are able to link those activities to individual users. In addition, the application is configured with an automated audit trail to track and monitor access.

CISP Compliant Wireless Settings

All communications sent from the TranScend™ Client Utilities and/or API's are encrypted from their point of origin, completely through the entire TranScend™ application. As Wireless Security is still evolving, INTRIX Technology, Inc. strongly recommends against using wireless transmission methods for sensitive transaction data. Unsecured wireless networks should never be used in conjunction with TranScend™ and any attempt to do so will result in an immediate Cease and Desist Order from INTRIX Technology, Inc.

In the event wireless networks must be utilized due to lack of infrastructure or wired networks, network administrators must ensure that available wireless security mechanisms be implemented to the fullest extent.

Wireless transmissions of cardholder data should be encrypted, over both public and private networks. Encrypt the transmissions by using Wi-Fi Protected Access (WPA) technology if WPA capable, or VPN or SSL at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are personnel changes.

If wireless technology is used within the payment environment, it should be implemented securely.

- Installation of perimeter firewalls between any wireless networks and the payment card environment, and configuration of these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment.
- Change wireless vendor defaults, including but not limited to, Wireless Equivalent Privacy (WEP) keys, default Service Set Identifier (SSID), passwords, and SNMP community strings, and disabling of SSID broadcasts. Enable Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.

Secure Remote Software Updates

In many instances, TranScend™ updates are delivered via remote access into customers' systems. In the event that a customer is required to use a modem to perform this action the following usage policies for critical employee-facing technologies, such as modems should be established. To define proper use of these technologies for all employees and contractors, ensure these usage policies require:

- Explicit management approval.
- Authentication for use of the technology.
- A list of all such devices and personnel with access.
- Labeling of devices with owner, contact information, and purpose.
- Acceptable uses of the technology.
- Acceptable network locations for these technologies.
- A list of company-approved products.
- Automatic disconnect of modem sessions after a specific period of inactivity.
- Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.

Alternatively, if software updates are received via VPN or other high-speed connection, customers are advised to properly configure a personal firewall product to secure "always-on" connections. This same policy of installing personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network should be followed.

Secure Remote Access To The Networks

If employees, administrators, or vendors can access the application remotely, access should be authenticated using a 2-factor authentication mechanism. Use technologies such as Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) with tokens or VPN with individual certificates.

Additionally, if INTRIX personnel are allowed to remotely access a customer's site for application support, the vendor should establish processes implemented to:

- Restrict access to passwords to authorized vendor personnel.
- Protect customers' passwords from unauthorized use.

- Establish customer passwords according to best practice (Previous Section).

In summary, customers who allow remote access to their networks should implement restrictive policies and use stringent security measures that govern remote access. Level 1 & 2 merchants should use a combination of unique username and complex password in addition to an additional item authentication (Token, etc.).

Level 3 merchants should use a combination of unique username and strong password in addition to highest security settings for remote access control software such as PCAnywhere, GoToMyPC, etc).

Secure Data

Do Not Store Cardholder Data On Internet Accessible Systems

Proper precautionary methods should be followed in securing access to the TranScend™ database and application. We recommend restricted physical and remote access to the server where the TranScend™ and/or database reside. Only the most trusted personnel should be given access to this database. All of the cardholder data is encrypted inside of the TranScend™ database, however, best practices dictates that both the payment application and database should not be stored on the same server or in the DMZ with the web server.

SSL & Secure Data Transmission Over The Internet

Information transmitted to the processors is required to be sent using SSL. In addition, it's required that data passed to TranScend™ or transmitted using the Internet as part of the network path must be sent using SSL. TranScend™ encrypts all data as it is transmitted throughout the application itself, but any cardholder information that travels across any network prior to entering the Tpa Client or one of the TranScend™ API mechanisms should also be transmitted using SSL.
Any sensitive data pulled from the application should never be sent via unencrypted e-mail. Public encryption tools such as PGP are recommended for use when transmitting this sensitive data. A copy of the application can be downloaded at http://www.pgp.com/products/desktop/personal/index.html.

Appendix F: PABP Compliance, Recommendations, and Requirements

Portions of the text below in this section was copied from the Version 1.4 January 2007 version of the VISA Cardholder Information Security Program (CISP) Payment Application Best Practices (PABP) document that can be downloaded from:
http://usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc

The information is included here primarily to point out how TranScend™ complies with the requirements as stated in that document as well as to illustrate the rigorous scrutiny that the application is subjected to. The information is provided here also to provide assist to vendors, integrators, or merchants with regards to evaluating the facts of the industry's requirements that TranScend™ must comply with. Finally, this information is provided so that merchants, integrators, or vendors adopting the use of the TranScend™ product can be provided with the specific recommendations and requirements for CISP and PABP compliant deployments of the system.

Relationship Between PCI DSS and PABP

The requirements for the PABP are derived from the Payment Card Industry Data Security Standard (PCI DSS) and the PCI DSS Security Audit Procedures. These documents, which can be found at www.pcisecuritystandards.org , detail what is required to be PCI DSS compliant (and therefore what a payment application must support to facilitate an application user's PCI DSS compliance) and should be used as a reference for the PCI DSS and supporting documentation.
Secure payment applications, when implemented in a PCI DSS-compliant environment, will minimize the potential for security breaches leading to compromises of full magnetic stripe data, card validation codes and values (CAV2, CID, CVC2, CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches.

Scope of PABP

The PABP applies to software vendors who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement. The PABP does not apply to payment software developed by merchants and agents if used only in-house (not sold to a third party), since this in-house developed payment software would be covered as part of the merchant's or agent's normal PCI DSS compliance.

NOTE: All validated payment application products must be general releases and not beta versions.

Data Retention Requirements

The following table (from the PCI DSS) illustrates commonly used elements of cardholder data and sensitive authentication data, whether storage of that data is permitted or prohibited, and whether this data needs to be protected. This table is not meant to be exhaustive; its sole purpose is to illustrate the different type of requirements that apply to each data element.

The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and the PABP. If PAN is not stored, processed, or transmitted, PCI DSS and PABP do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVVS/CID	NO	N/A	N/A
	PIN/ PIN BLOCK	NO	N/A	N/A

** These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*

*** Do not store sensitive authentication data subsequent to authorization (not even if encrypted).*

PABP Implementation Guide

Validated applications must be capable of being implemented in a PCI DSS-compliant manner. Software vendors are required to provide a PABP Implementation Guide to instruct their customers and resellers/integrators on secure product implementation, to document the secure configuration specifics mentioned throughout this document, and to clearly delineate vendor, reseller/integrator, and customer responsibilities for meeting PCI DSS requirements. It should detail how the customer and/or reseller/integrator should enable security settings within the customer's network, (for example, the PABP Implementation Guide should cover responsibilities and basic features of PCI DSS password security even if this is not controlled by the application, so that the customer or reseller /integrator understands how to implement secure passwords for PCI DSS compliance).

Payment applications, when implemented according to the PABP Implementation Guide, and when implemented into a PCI DSS compliant environment, should facilitate and support customers' PCI DSS compliance.

Qualified Payment Application Security Professional (QPASP) Requirements

- Only Qualified Payment Application Security Professionals (QPASP) employed by Qualified Payment Application Security Companies (QPASC) are allowed to perform PABP audits. Please refer to the Qualified Payment Application Security Company (QPASC) list at www.visa.com/cisp for more information.
- The QPASP must utilize the testing procedures documented in this Payment Application Best Practices document.
- Both QPASP and software vendor must complete and sign the Confirmation of Report Accuracy letters (available at www.visa.com/cisp) and submit to Visa USA in a secure manner along with the Report on Validation.
- Once compliant, Visa will include the software vendor and product version in the Validated Payment Application List at www.visa.com/cisp **for one year only**. The expiration date will be determined by the date that Visa approves the Report on Validation. Visa will send an acceptance letter to software vendors indicating approval of the report. Software vendors must re-validate their application for PABP compliance utilizing a QPASP if they wish to be "active" on the Visa website. Otherwise, Visa will remove the software vendor's listing from the website if re-validation is not received by the due date (please refer to Re-Validation section).

Testing Laboratory

The software vendor must have a working, semi-production laboratory where the validation process is to occur. The laboratory must include the following:

- All common implementations (including region/country specific versions) of the payment application to be tested.
- Implementation of security devices. At a minimum, the following must be running per PCI DSS requirements: firewall or traffic filtering devices, Network Address Translators (NAT), Port Address Translators (PAT), anti-virus software and encryption.
- Establishment of PCI DSS compliant operating systems and applications necessary to run the software.

The laboratory implementation must include all systems where the application is implemented. For example, a standard implementation of software vendor's payment application might include a client/server environment within a retail storefront, and back office or corporate network. The laboratory must simulate the total implementation. It is required that the laboratory is capable of simulating and validating all functions of the software, to include generation of all error conditions and log entries.

NOTE: Alternatively, the software vendor may elect to have the validation performed at the QPASC's laboratory provided that the above requirements are met.

Instructions and Content for Report on Validation

This document is to be used by QPASP's as the template for creating the Report on Validation and must be submitted to Visa securely. All software vendors and product versions which have validated full compliance

with PABP will be included on the list of validated payment applications published at www.visa.com/cisp. No software vendor and product version will be included until all PABP controls are validated to be Comment.

All QPASP's must follow the instructions for report content and format when completing a Report on Validation.

Executive Summary

Include the following:

- Software vendor name
- Software vendor contact information
- Software vendor mailing address
- QPASP name and contact information
- Product Name
- Product Version (if applicable)
- List of resellers and/or integrators for this product
- Operating system with which the payment application was tested. Include other applications required by the payment application.
- Database software used or supported by the application.
- Brief description of the payment application/family of products (2-3 sentences)
- Brief description of the software vendor or QPASC's laboratory (2-3 sentences)
- A network diagram of a typical implementation of the software (not necessarily a specific implementation at a merchant's site) that includes, at high-level, connections into and out of a merchant's network and the implementation components within the merchant's network, including implementation of POS devices, systems, databases, and web servers as applicable
- Describe/diagram each piece of the communication link, including 1) LAN, WAN or internet, 2) host to host software communication, and 3) within host where software is deployed (e.g. how two different processes communicate with each other on the same host)
- All flows of cardholder data
- All payment application related software components, including third party software dependencies
- End to end authentication, including application authentication mechanism, authentication database, and security of data storage
- Describe the typical merchant that this product is sold to (for example, large, small, if industry-specific, Internet, brick-and-mortar) and vendor's customer's base. (e.g. market segment, big customer names).

Description of Scope of Validation and Approach Taken

- Describe scope of review as defined at Scope of Assessment, above
- Describe region/country specific implementations covered
- Timeframe of validation
- List of documentation reviewed

Findings and Observations

- All QPASPs must use the following template to provide detailed report descriptions and findings
- Describe tests performed other than those included in the testing procedures column.

Contact Information and Report Date

- Software vendor contact information (include URL, phone number and email address)
- QPASP contact information (include phone number and email address)
- Date of report

Re-Validation

No change - Visa does NOT currently require re-validation for previously validated product versions if *no* changes were made to the compliant payment application version. However, Visa will require a Confirmation of Report Accuracy from the software vendor prior to the expiration date indicating that *no c*hanges were made to the validated payment application.

Changes made do not affect any of the 14 PABP requirements - If changes were made to a previously validated payment application version but do not impact the compliance of any of the 14 PABP requirements, Visa will require the software vendor to submit a description of each change in addition to a Confirmation of Letter Accuracy indicating so.

Major changes and product version upgrade – Changes made to a previously validated payment application version which impact any of the 14 PABP requirements will require a completely new and separate PABP validation performed by a QPASP. All PABP validation requirements apply.

Definitions

The following definitions pertain to the Validation Procedures and Reporting:

Best Practices – Recommended practices for software vendor to create secure payment applications to help their customers comply with CISP.

- **Testing Procedures** – A process to be followed by an independent security audit firm to address individual Best Practices and testing considerations

- **Comment** - Please provide a brief description of Best Practices found to be Comment. If a Best Practice is Not Applicable to the software, please explain why and define where this control should be implemented (e.g. this server-based control is the customers' responsibility).
- **Not Comment** – Please provide a brief description of Best Practices that are not Comment.
- **Target Date/Comments** – For those Best Practices "Not Comment" include a target date that the application vendor expects to have "Comment." Any additional notes or comments may be included here as well.

PABP Requirements

PABP Requirements	Comment
1.1 Do not store sensitive authentication data subsequent to authorization (even if encrypted): Sensitive authentication data includes the data as cited in the following requirements 1.1.1 through 1.1.3: **PCI Data Security Standard 3.2**	See sections for more details. However, as a matter of course **TranScend™** does NOT store any of these data types IN ANY FORM FOR ANY REASON.
1.1.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. *In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.* ***NOTE:** See PCI DSS Glossary for additional information.* **PCI Data Security Standard 3.2.1**	**TranScend™** NEVER stores TRACK data for any reason. However, in some cases it is important to know whether or not TRACK data WAS PRESENT at the time the transaction was created. For this reason, **TranScend™** will do the following: If TRACK data WAS PRESENT on the transaction, then **TranScend™** WILL store an 'N' character at each location where a digit was present in the TRACK and an 'A' character at each location where an alpha-character was present in the TRACK. If NO TRACK was present on the transaction, then **TranScend™** will store NA (Not Assigned) for that data element.
1.1.2 Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. ***NOTE:** See PCI DSS Glossary for additional information.* **PCI Data Security Standard 3.2.2**	**TranScend™** NEVER stores CVV data for any reason. However, if CVV WAS PRESENT with the transaction when it was created, then **TranScend™** will store an 'N" for each digit present at the time the transaction was created. If the CVV was NOT PRESENT, then **TranScend™** will store a value of 'NA' (Not Assigned) for the data value.

1.1.3 Do not store the personal identification number (PIN) or the encrypted PIN block. *PIN blocks must never be retained (even if encrypted) after transaction authorization.* **PCI Data Security Standard 3.2.3**	**TranScend™** NEVER stores PIN data for ANY REASON.
1.1.4 Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the software. **PCI Data Security Standard 3.2**	**TranScend™** HAS NEVER STORED any of these DATA ITMEMS outside of the methods described. See comments for sections 1.1.1, 1.1.2, and 1.1.3. As such, THERE ARE NO ACTIONS OF THIS TYPE REQUIRED.
1.1.5 Securely delete any cryptographic key material or cryptogram stored by previous versions of the software. This could be cryptographic keys used for computation or verification of cardholder data or sensitive authentication data.	**TranScend™** has ALWAYS utilized a completely PRIVATE KEY ENCRYPTION scheme. Therefore there is NO KEY MATERIALS(s) OF ANY KIND that NEED to be DESTROYED.

1.1.6 Securely delete any log files, debugging files, and other data sources received from customers for debugging or troubleshooting purposes, to ensure that magnetic stripe data, card validation codes or values, and PINS or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use. **PCI Data Security Standard 3.2**	ALL log files produced by **TranScend™** will NEVER expose ANY of the mentioned data elements (or ANY OTHER CARD holder DATA). There is NO SETTING that could cause the application to OUTPUT SUCH values IN ANY FORM. Therefore, it IS NOT POSSIBLE for DATA of THIS TYPE to GATHERED or SENT in ANY FASHION. SPECIAL NOTE TO: Vendors/Integrators. IF YOUR APPLICATIONS ALLOW STORAGE OF THESE DATA ELEMENTS, are hereby advised of this requirement here and are strongly urged to adopt this policy with regards to HANDLING of DATA of this type. The FOLLOWING ADDITIONAL GUIDANCE is PROVIDED: • Resellers/integrators must collect sensitive authentication only when needed to solve a specific problem • Resellers/integrators must store such data only in specific, known locations with limited access • Resellers/integrators must collect only the limited amount of data needed to solve a specific problem • Resellers/integrators must encrypt sensitive authentication data while stored • Resellers/integrators must securely delete such data immediately after use.
2.1 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). ***NOTE:*** *This requirement does not apply to those employees and other parties with a specific need to see full PAN; nor does the requirement supersede stricter requirements Comment for displays of cardholder data (for example, for point of sale [POS] receipts).* ***PCI Data Security Standard 3.3***	**TranScend™** ALLOWS PAN masking to be established on a PER USER basis at the time the user is created (or when the user is edited). If a user has been assigned a PAN mask, then there is NO WAY that the user WILL EVER SEE a non-masked PAN. In NO CASE is a NON-MASKED PAN ever displayed on any receipts; regardless of the PAN-masking level for the user whose terminal produces the receipt.

2.2 Render PAN, at a minimum, unreadable anywhere it is stored, (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches: Strong one-way hash functions (hashed indexes) Truncation Index tokens and pads (pads must be securely stored) Strong cryptography with associated key management processes and procedures. The MINIMUM account information that needs to be rendered unreadable is the PAN. **PCI Data Security Standard 3.4** *The PAN must be rendered unreadable anywhere it is stored, even outside the payment application.*	The PAN is NEVER stored in clear-text in ANY location. The ONLY places where PAN data is stored (BUT ONLY AFTER ENCRYPTION with 128-bit AES) is in the main system database and in database-recovery log-files produced by **TranScend™**.
2.3 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (e.g. not using local system accounts). Decryption keys cannot be tied to local user accounts. **PCI Data Security Standard 3.4.1**	**TranScend™** DOES NOT USE this technique in ANY manner.
2.4 Application must protect encryption keys used for encryption of cardholder data against disclosure and misuse. **PCI Data Security Standard 3.5**	**TranScend™** utilizes a PRIVATE KEY ENCRYPTION system wherein EACH FIELD that is encrypted is UNIQUELY ENCRYPTED with one of 3e18 possible keys. The KEY used for the PER FIELD ENCRYPTION OPERATION is COMPUTED at runtime. There is NO EXTERNAL KEY schedule.

2.5 Application must implement key management processes and procedures for keys used for encryption of cardholder data. **PCI Data Security Standard 3.6**	See comment in section 2.4 above.

3.1 Application must require unique usernames and complex passwords for all administrative access and for all access to cardholder data. **PCI Data Security Standard 8.1 and 8.2** ***NOTE:*** *These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.*	When users are created a STRONG password is REQUIRED. If a STRONG password is NOT DETECTED the application WILL NOT ACCEPT the attempted entry. ALL usernames and passwords are REQUIRED by database indexes to be UNIQUE. In addition, **TranScend™** DOES NOT RELY ON or MAKE USE of BUILT IN administrative accounts (such as the 'sa' DBMS or other PRIVILEGED OPERATING SYSTEM USERS). Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt this policy with regards to all other forms of access to any system related to, or that has any potential access to, the **TranScend™** database. In addition, the following additional guidance is provided: 1. No deployment should make use of administrative accounts for application logins, for example, don't use the "sa" account for application access to the database. 2. All deployments should use strong passwords for any default accounts, and then disable or do not use the accounts. 3. Do not use group, shared, or generic accounts and passwords. 4. The **TranScend™** client will limit access to the application upon repeated access attempts by locking out the user ID after not more than six attempts. Whenever possible, these same techniques should be applied to all means to access systems that have any possible connection to the **TranScend™** system and should set the lockout duration to no less than 30 minutes or until administrator enables the user ID. 5. If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal. For example, make use of password locked screen savers for all user sessions with the Operating System

3.2 Access to PCs, servers, and databases with payment applications must require a unique username and complex password. **PCI Data Security Standard 8.1 and 8.2**	See comment in section 3.1 above for **TranScend™** application requirements with regard to this requirement. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt this policy with regards to all other forms of access to any system related to, or that has any potential access to, the **TranScend™** database.
3.3 Encrypt application passwords. **PCI Data Security Standard 8.4**	ALL **TranScend™** USER passwords are NEVER DIRECTLY STORED. Rather, the "raw-password" is input into a multiple-pass oscillating MD-5 algorithm. The output of that algorithm is stored in the user record. There is an optional utility for **TranScend™** where the vendor can define their own user (within the **TranScend™** dbms) for use by the **TranScend™** processes. If that utility is used, then the username and password selected by the user is ENCRYPTED using a 128-bit BLOWFISH and that value is stored in the system registry in order that the **TranScend™** process can utilize the customized application password.
4.1 Application must log all user access (especially users with administrative privileges), and be able to link all activities to individual users. **PCI Data Security Standard 10.1**	The "security" log produced by the **TranScend™** system LOGS ALL SUCCESSFUL logons and FAILED-LOGON attempts. ALL transaction records within **TranScend™** require a USER-ID field on the record. This requirement is reinforced by the application code as well as by foreign keys on the database tables.
4.2 Application must implement an automated audit trail to track and monitor access. **PCI Data Security Standard 10.2 and 10.3**	The "security" log produced by the **TranScend™** system LOGS ALL SUCCESSFUL LOGONS AND FAILED LOGON ATTEMPTS. In addition, the system maintains an "audit" log for ALL ACTIVITIES related to "monetary events" which have the USER-ID on these log records.

5.1 Develop all web applications based on secure coding guidelines such as the *Open Web Application Security Project* guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include: **PCI Data Security Standard 6.5**	**TranScend™** is NOT a web-based application. However, there is nothing to preclude it being designed into such a solution. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration of **TranScend™** into this kind of deployment.
5.1.1 Invalidated input.	ALL data arriving into the CLIENT or API functions are FULLY VALIDATED and SANITY checked to the maximum degree possible.
5.1.2 Broken access control (e.g., malicious use of user IDs).	**TranScend™** allows for the IMMEDIATE DE-ACTIVATION of USER ACCOUNTS from the Administrative screens. ONCE a USER has been DE-ACIVATED, they CAN NOT LOG ON AGAIN.
5.1.3 Broken authentication and session management (use of account credentials and session cookies).	This scenario IS NOT POSSIBLE in the **TranScend™** application. Each "outward" (or client facing) connection into the system is INTEGRITY CHECKED PRIOR TO ANY USE of the data channel. IF there is ANY ISSUE detected in the channel, then the SESSION IS TORN DOWN IMMEDIATELY and CAN NOT BE USED. In this case, the CLIENT side of the CONNECTION MUST BE RE-CREATED. There IS NO DATA OR STATE RETAINED FROM THE PREVIOUS CONNECTION.
5.1.4 Cross-site scripting (XSS) attacks.	Is Not Applicable to **TranScend™**
5.1.5 Buffer overflows.	**TranScend™** makes NO USE of FIXED SIZE BUFFERS on any EXTERNAL ACCESS POINTS (including all API and functions used by ANY CLIENT). Rather, BUFFERS of the REQUIRED SIZE are ALLOCATED for EACH and EVERY REQUEST.
5.1.6 Injection flaws (e.g., SQL injection).	Is Not Applicable to **TranScend™**
5.1.7 Improper error handling	**TranScend™** makes use of techniques that we refer to as FAIL-FAST TECHNIGUES. These techniques are applied in the following manner: For DATA COMMUNCTIONS: HEAVY USE of SEVERAL LAYERS of MESSAGE ERROR DETECTION and VALIDATION techniques. If ANY ANOMOLOUS CONDITION is DETECTED, the CONNECTION is IMMEDIATELY TORN DOWN. ANY PROCESS which detects ANY ANOMOLOUS INTERNAL CONDITION will IMMEDIATELY EXIT in response to that condition.

5.1.8 Insecure storage	**TranScend™** MAKES NO USE OF INSECURE STORAGE. All data of any sensitive nature is stored in DATABASES.
5.1.9 Insecure configuration management.	ALL CONFIGURATION SCREENS within the **TranScend™** system IS PROTECTED AND IS ONLY AVAILABLE to ADMINISTRATIVE USERS. If a user IS NOT an ADMINISTRATIVE USER then THEY WILL HAVE NO ACCESS to System CONFIGURATION SCREENS.
5.2 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle. **PCI Data Security Standard 6.3**	DATA SECURITY is, and always has been, a FUNDAMENTAL CONSIDERATION for all design decisions. In NO EVENT, will ANY other consideration OUTWEIGH the NEED for data security at every level.
5.2.1 Testing of all security patches and system and software configuration changes before deployment	This type of testing is part of our written test plans. In addition, these test plans are frequently reviewed and extended whenever required. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.2.2 Separate development, test, and production environments	The **TranScend™** Development Team has a dedicated QA test staff in addition to the development staff that creates the product. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.2.3 Separation of duties between development, test, and production environments	See comment above for section 5.2.2 Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.2.4 Live PANs are not used for testing or development	The development and test teams have test accounts provided by the processor companies that we partner with. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.

5.2.5 Removal of test data and accounts before production systems become active.	This requirement is not applicable to **TranScend™** development team. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.2.6 Removal of custom application accounts, usernames, and passwords before applications are released to customers.	**TranScend™** does not make use of any of these types of items. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.2.7 Review of custom code prior to release to customers, to identify any potential coding vulnerability.	This type of testing is part of our written test plans. In addition, these test plans are frequently reviewed and extended whenever required. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.3 Software vendor must follow change control procedures for all product software configuration changes. The procedures must include the following: **PCI Data Security Standard 6.4**	The **TranScend™** Development staff utilizes a software development approach that utilizes both long-standing and emerging recommendations for effective software development. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.
5.4 Disable or remove unnecessary and insecure services and protocols (e.g., NetBIOS, file-sharing, Telnet, unencrypted FTP, and others). These services and protocols must not be used or required by the application. **PCI Data Security Standard 2.2.2**	End users perform their own installations on systems within their enterprise. We have control over the practices in place at these end user facilities. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.

5.5 Ensure that all web-facing applications are protected against known attacks by either of the following methods: Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security. Installing an application-layer firewall in front of web-facing applications. PCI Data Security **Standard 6.6** ***NOTE:*** *For PCI DSS, this method is considered a best practice until June 30, 2008, after which it becomes a requirement.*	This requirement is not applicable to **TranScend™** development team. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**.

Protect Wireless Transmissions

PABP Requirement	Comment
6.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following: Use with a minimum 104-bit encryption key and 24 bit-initialization value. Use ONLY in conjunction with Wi-Fi Protected Access (WPA or WPA2) technology, VPN, or SSL/TLS. Rotate shared WEP keys quarterly(or automatically if the technology permits) Rotate shared WEP keys whenever there are changes in personnel with access to keys. Restrict access based on media access code (MAC) address. **PCI Data Security Standard 4.1.1**	Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™.**

Test Applications to Address Vulnerabilities

PABP Requirement	Comment
7.1 Software vendors must establish a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet), to test their applications for vulnerabilities, and for timely development and deployment of security patches and upgrades. Updates and patches must be delivered in a secure manner with a known chain-of-trust. Any underlying software or systems that are provided along with the payment application (e.g., web servers) must be included in this process. **PCI Data Security Standard 6.2**	Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™.**

Facilitate Secure Network Implementation

PABP Requirement	Comment
8.1 The payment application must be able to be implemented into a secure network environment. Application must not interfere with use of network address translation (NAT), port address translation (PAT), traffic filtering network devices, anti-virus protection, patch or update installation, or encryption. **PCI Data Security Standard 1, 3, 4, and 5**	**TranScend™** makes use of simple TCP/IP socket connections for all data exchanges. After the socket connection is established, then each end-point of this data channel participates in the formation of secured (encrypted) session for the duration of that data exchange. There is nothing in the **TranScend™** data exchange protocol that will encumber or otherwise inhibit any of the networking strategies listed in this requirement.

Cardholder Data Must Never Be Stored on A Server Connected To The Internet

PABP Requirement	Comment
9.1 The payment application must not require that the database server and web server be on the same server, or in the DMZ with the web server. **PCI Data Security Standard 1.3 and 1.3.4**	**TranScend™** is developed to support fully distributed deployment models, and as such makes no assumptions or requirements regarding the hosts that participate in the deployed system and the number and types of hosts involved.

Facilitate Secure Remote Software Updates

PABP Requirement	Comment
10.1 If software updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on modem only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a personal firewall product to secure "always-on" connections. **PCI Data Security Standard 1.3.9 and 12.3.9**	**TranScend™** DOES NOT EMPLOY any type of PUSH TECHNOLOGIES to perform UPDATES. Rather, any updates that would be applied to the customer's system is delivered via HTTP connection. IN ALL CASES, the CUSTOMER WILL INITIATE the UPDATE using a customized UPDATE PROCESS utilized by INTRIX for this purpose. Therefore, in order TO ENABLE the operation of the UPDATE application, the end-user MUST ONLY CONFIGURE their FIREWALL provide OUTBOUND CONNECTIONS on the HTTP STANDARD PORT 80. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**. For more information on this topic the reader is referred to Appendix G in this document.

Facilitate Secure Remote Access to Application

PABP Requirement	Comment
11.1 The payment application must not interfere with use of a two-factor authentication mechanism. The application must allow for technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates. **PCI Data Security Standard 8.3**	**TranScend™** does not have any mechanism that would prevent or preclude such mechanisms for remote access and control. Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**. For more information on this topic the reader is referred to Appendix G in this document.
11.2 Remote access must be authenticated using a two-factor authentication mechanism. **PCI Data Security Standard 8.3**	Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**. For more information on this topic the reader is referred to Appendix G in this document.
11.3 If vendors, resellers/integrators, or customers can access customers' applications remotely, the remote access software must be implemented securely. **PCI Data Security Standard 8.3**	Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**. For more information on this topic the reader is referred to Appendix G in this document. The following additional guidance is also provided: • Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer) • Allow connections only from specific (known) IP/MAC addresses • Use strong authentication or complex Passwords for logins • Enable encrypted data transmission • Enable account lockout after a certain number of failed login attempts • Configure the system so a remote

	user must establish a Virtual Private Network (“VPN”) connection via a firewall before access is allowed • Enable the logging function • Restrict access to customer Passwords to authorized reseller/integrator personnel • Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, 8.5.

Encrypt Sensitive Traffic Over Public Networks

PABP Requirement	Comment
12.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and, internet protocol security (IPSEC)) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).* **PCI Data Security Standard 4.1**	ALL inter-process data exchanges between ANY **TranScend™** processes IS ALWAYS PERFORMED over a SECURE SESSION utilizing 128-bit CRC-checked Blowfish ENCRYPTION for all data packets sent between the two endpoints.
12.2 The application must never send unencrypted PANs by e-mail. PCI Data Security Standard 4.2	ALL data exchanges between **TranScend™** processes always use secure sessions prior to ANY EXCHANGE of data. **TranScend™** DOES NOT EMPLOY ANY MEANS wherein PAN data could be sent via E-Mail.

Encrypt All Non-Console Administrative Access

PABP Requirement	Comment
13.1 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. **PCI Data Security Standard 2.3** *Telnet or rlogin must never be used for non-console administrative access.*	Merchants/Vendors/Integrators are hereby advised of this requirement here and are strongly urged to adopt these policies with regards to the integration and deployment of **TranScend™**. The following additional guidance is provided: It is recommended that only encrypted data channels should be used for all non-console administrative access. Use technologies such as SSH, VPN or SSL/TLS for encryption of non-console administration.

Maintain Instructional Documentation and Training Programs for Customer, Resellers, and Integrators

PABP Requirement	Comments
14.1 Develop, maintain, and disseminate a PABP Implementation Guide(s) for customers, resellers, and integrators that accomplishes the following:	This requirement is the very reason that this information is included in this documentation.
14.1.1 Addresses all requirements in this document wherever the PABP Implementation Guide is referenced.	**TranScend™** has undergone extensive internal reviews and 3rd Party Confirmation as being compliant with these requirements.
14.1.2 Includes a review at least annually and updates to keep the documentation current with software changes as well as with changes to the requirements in this document.	Documentation Reviews and Revisions as required are part of the regression test plan for the **TranScend™** product.
14.2 Develop and implement training and communication programs to ensure software resellers and integrators know how to implement the application software and related systems and networks in a PABP-compliant manner. Update the training on an annual basis and whenever new software versions are released.	This requirement is the very reason that this information is included in this documentation.

Appendix G: Lin.exe Usage

Introduction to the Lin.exe Utility

Lin (short for Let In) is a tool that allows users the capability to manage their louts.intrix file (the Lock Outs database file that is created and managed by the data server).

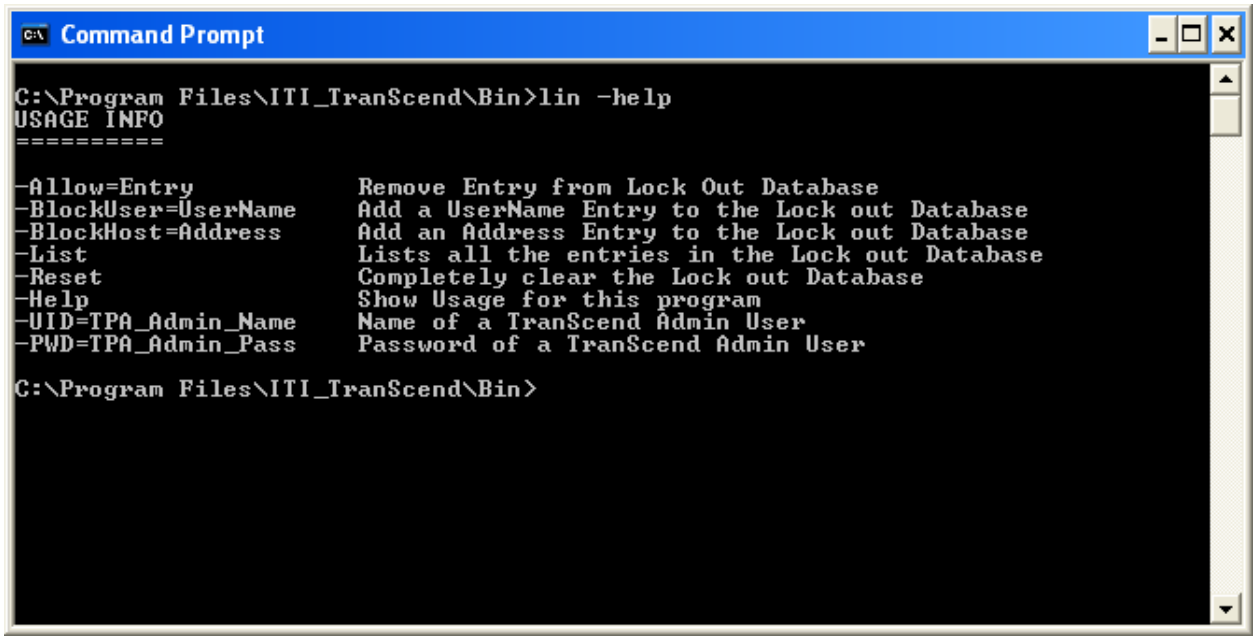
Some preliminary bits of info on the louts contents:

1. PABP requires that users be locked out for no less than 0.5 hours when they are locked out due to failing correct password entry. As such, whenever a USER is locked out from the client in this manner, the "user lock out record" will be automatically expired by the data server as it runs.
2. PABP has NO REQUIREMENT to lock out workstations (ip addresses). However, in analyzing the security threat from password attacks, we determined that continued failed password attempts from a workstation implies that the workstation itself is NOT PROPERLY SECURED. So, TranScend exceeds the required standard by also locking out workstation addresses.
3. Workstation Lockouts DO NOT AUTOMATICALLY EXPIRE and MUST BE MANUALLY ALLOWED by the system administrator.

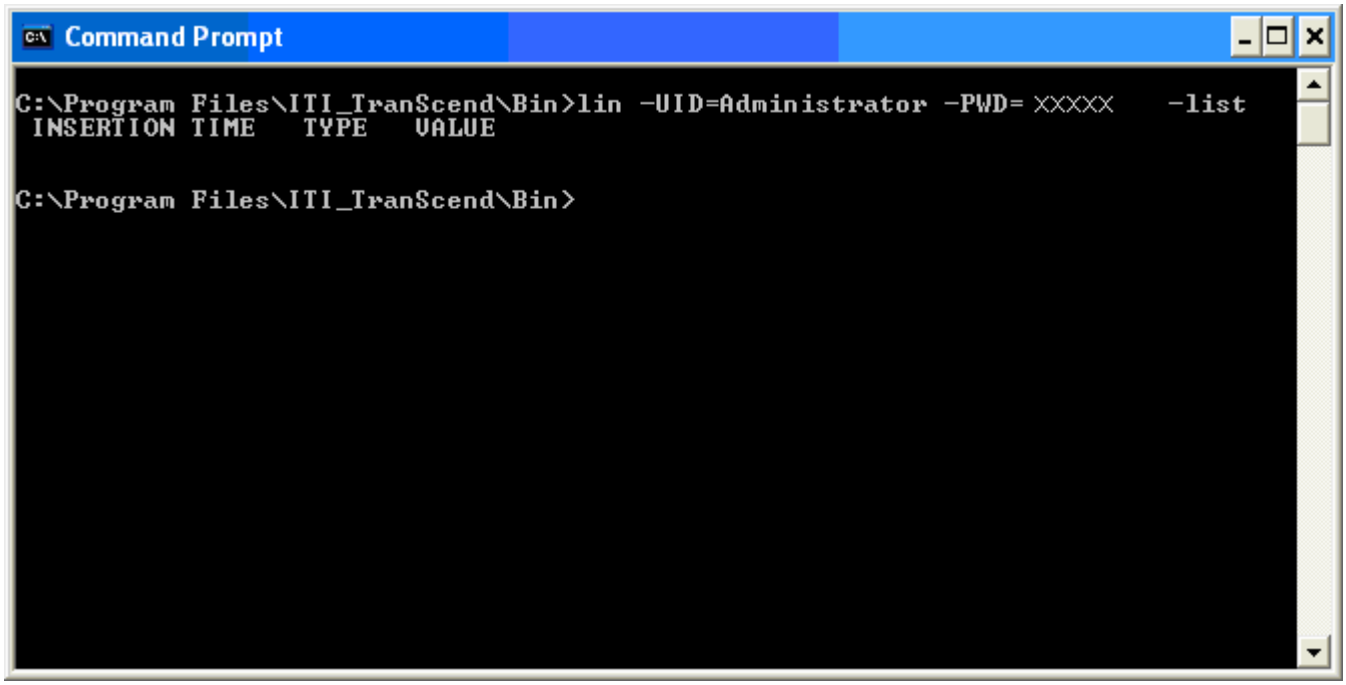
The lin.exe program is a command line utility. As such it runs in a command shell window. So, to experiment with lin, first open a cmd window and cd to "/program files/ITI_TranScend/bin".

The following examples will show ways that you would use the lin.exe program.

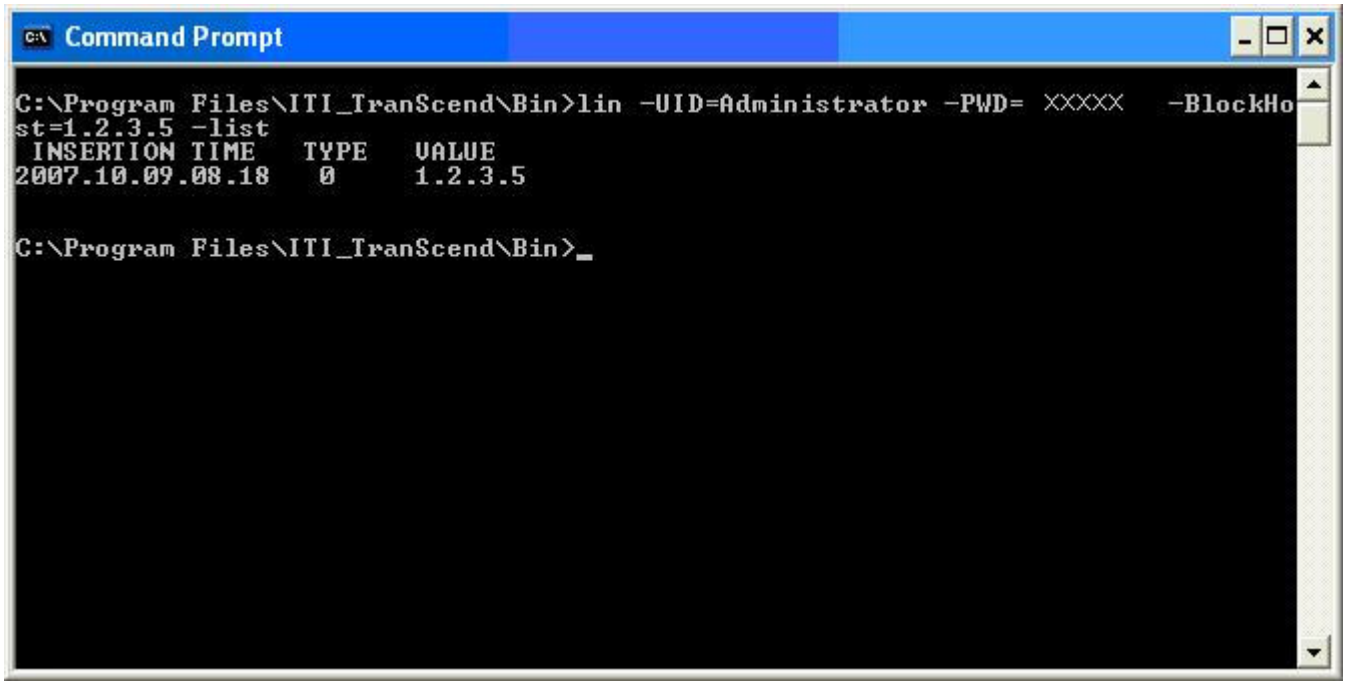
If you enter the command "lin -help", you will see usage information for the program.



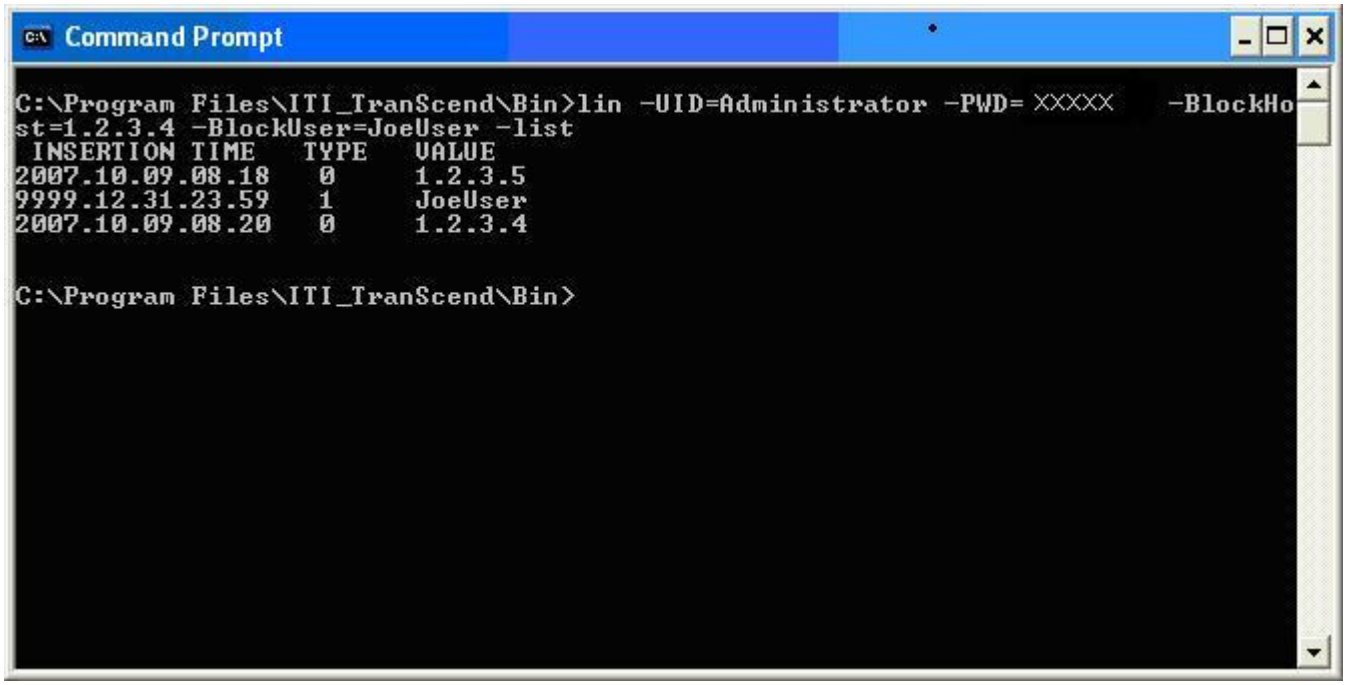
If you enter "lin -UID=Administrator -PWD=xxxxx -list", you will see the contents of the lock out database. The sample shown below is for an empty lockout database.



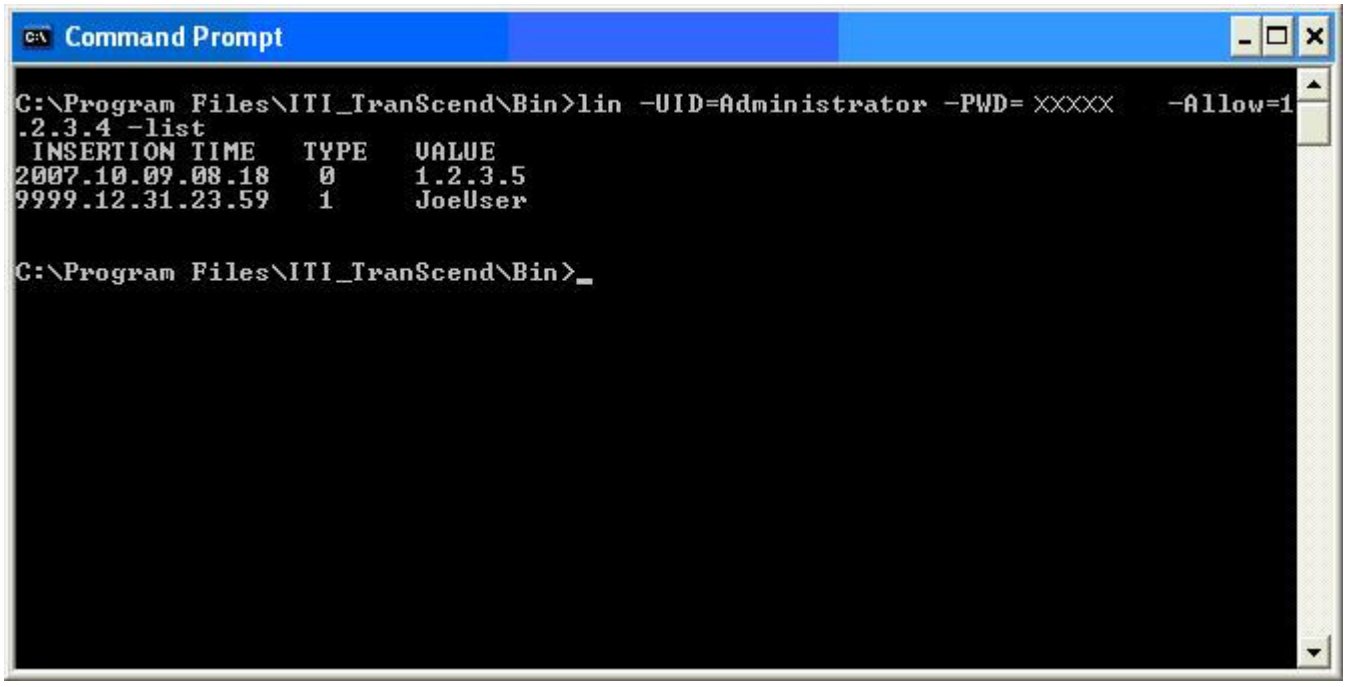
If you enter “lin -UID=Administrator -PWD=xxxxx -BlockHost=1.2.3.5 -list”, you will see that you have added a blocked address to the lock out database.



If you enter “lin -UID=Administrator -PWD=xxxxx -BlockHost=1.2.3.4 -BlockUser=JoeUser -list”, you will see that you have added a blocked user (type is 1) and a blocked host address (type is zero). Also, notice that if you manually block a user using lin.exe, then notice that the insertion time is far off into the future. This is on purpose so that record will NEVER EXPIRE. The thinking here is that if you are manually adding someone to your lock out database, that you very likely really do want that user blocked “forever.” So, this behavior exceeds the PABP standard for minimum lock out time for users.



If you enter “lin -UID=Administrator -PWD=xxxxx -allow=1.2.3.4 -list”, you will see that you have removed an entry from the lock out database. Note that the allow command can be used to allow users and/or addresses. In other words, the allow command can be used to allow both users and addresses. After this, you can see that when the database is listed, the entry 1.2.3.4 has been removed, but the user entry still remains.



If you enter “lin -reset -list”, you will see that you have erased all entries in the lock out database with the reset command. When the database is listed you can see that it is empty again.

Appendix H: Optional Utilitity to Set Customized Database System Password

Below (see Figure One) you will see the window for the database user/password utility program. This program is used to alter the user name and password that will be used by the TPA Data Security Server when it connects to the database server (dbms).

IMPORTANT NOTE: This uitlity should only be run on the host where the Data Security Server process of the TPA transaction processing system. The reasons for this requirements are:

1. This utility will utilize the DSN and other connection information to add a new user to the dbms used by TPA.
2. This utility will add command line arguments used by the data server so that the process can utilize the new customized user information specified by the user of this utility.

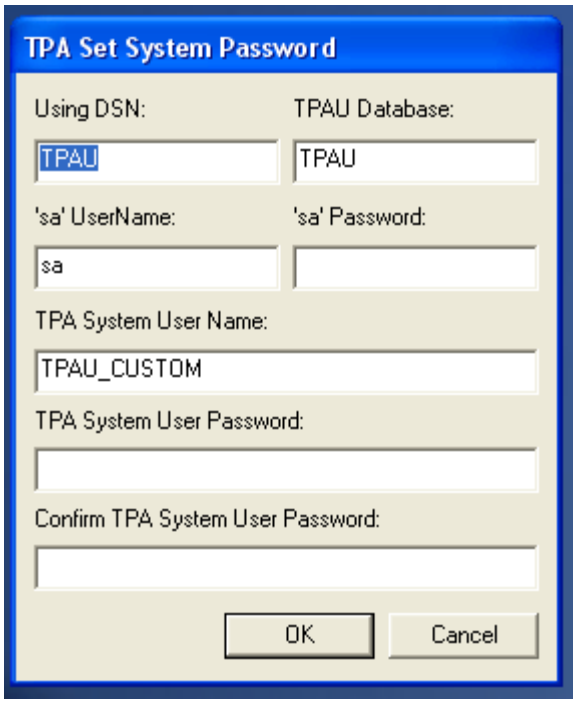


Figure One.

As you can see some of the fields are set with 'system defaults' a a convenience to the user. Each of these settings will be explained in the following section.

- **Using DSN:** This is the System DSN (see ODBC Administrator Appliet in Control Panel) that defines the dbms used by TPA. If you have not altered your System DSN after your installation, then the default setting of TPAU should work.
- **TPAU Database:** This is the name of the main TPA database used by the sytem. If you have not altered your default database after your installation, then the default setting of TPAU should work.
- **'sa' UserName:** This is where the user will have to enter a valid 'sa' user in the dbms used by TPA. See your database system administrator if you do not know a valid 'sa' user on your system.
- **'sa' Password:** This is where the user will have to enter a valid password for the 'sa' user. If you do not know a valid password, then you must consult with the database system administrator.

- **TPA System User Name:** This is where the user will enter a *NEW USER NAME* that will be used by TPA to connect to the dbms.
- **TPA System User Password and Confirm TPA System User Password:** These two fields are where the *NEW USER PASSWORD* for the *NEW TPA USER* will be entered. The password is entered twice to allow the user to confirm the value that will be used.

NOTE: If the User Password and the Confirmation of the same do not match, then the program will display a message-box to that effect so that user can correct this error.

End Effect of Using This Utility

- The NEW USER will be added as a valid login to the database that is 'behind' the DSN entry.
- This can be proven by looking at Enterprise Manager (or similar utility).
- In looking at Figure Two below, you can see that a new login was created by the utlity.

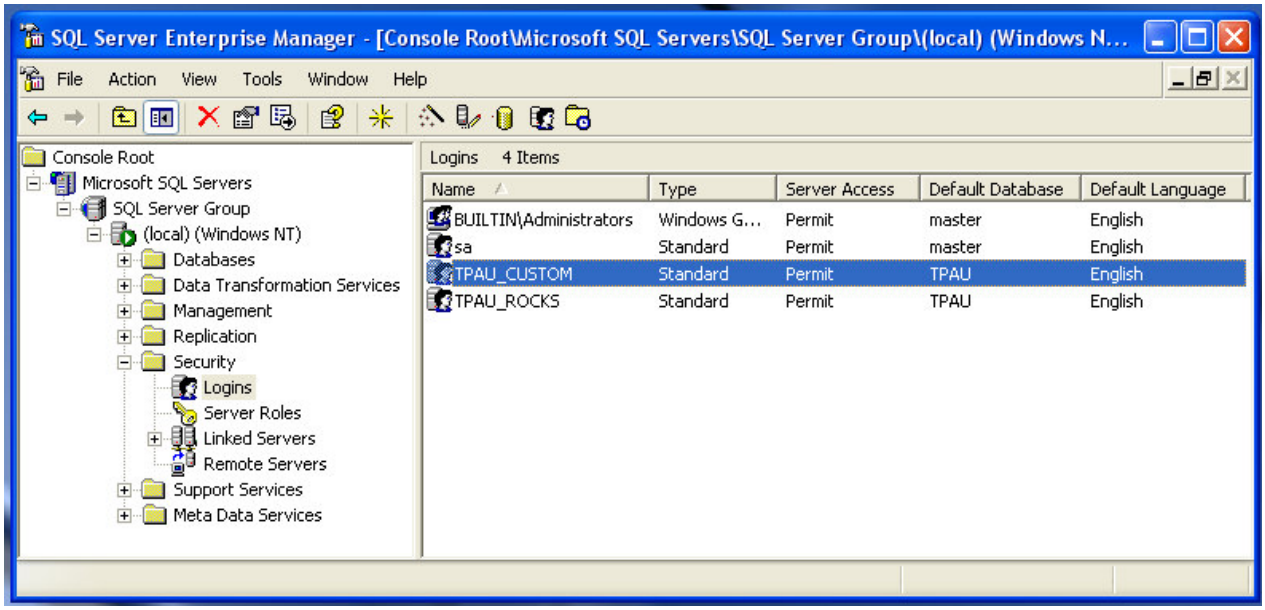


Figure Two

- The login exists at the database server level.
- In order for the a login to have access to any single database within the server, the user must be added to that database.
- The utility program also performs this task.
- The NEW USER will be added to all the TPA databases that are installed on the system.

See Figure Three below for an example of this.

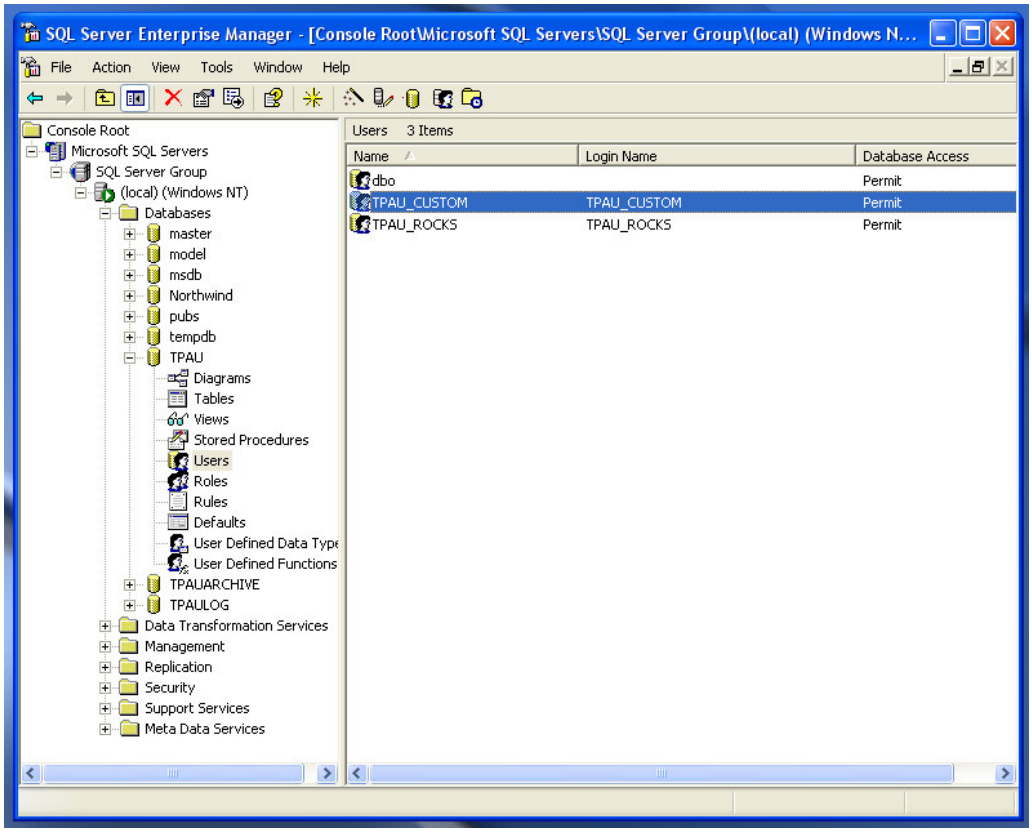


Figure Three

From the figure above, you can see that the NEW USER was also added as a user to the TPAU database. The user will also be added to the TPAUARCHIVE database and to the TPAULOG if that database is present. Using the utility performs all the tasks necessary to provide your TPA system with a custom user.

NOTE: About System Security. The NEW USER and NEW USER PASSWORD are stored in an encrypted from in the system registry. These values are encrypted with a key based on the hardware signature of your server. This additional level of security prevents anyone from trying to replace this information with fraudulent values in order to gain access to your company's data.

In order to make this security enhancement complete, the encrypted values for the NEW USER and NEW USER PASSWORD must be used by the TPA Data Server to connect to the database engine (dbms). See Figure Four below for a sample of how this is done. From the figure you can see that we are looking at the command line used by the TPA Data Server. You can also see that the new run-line values for WithDbUid and WIthDbPwd has been added to the command line. The encrypted values for the entries are stored here. The data server will (if it finds these entries on the run-line) will decrypt the values using a key based on the hardware signature of the host machine. It will then use the decrypted values to connect to the dbms.

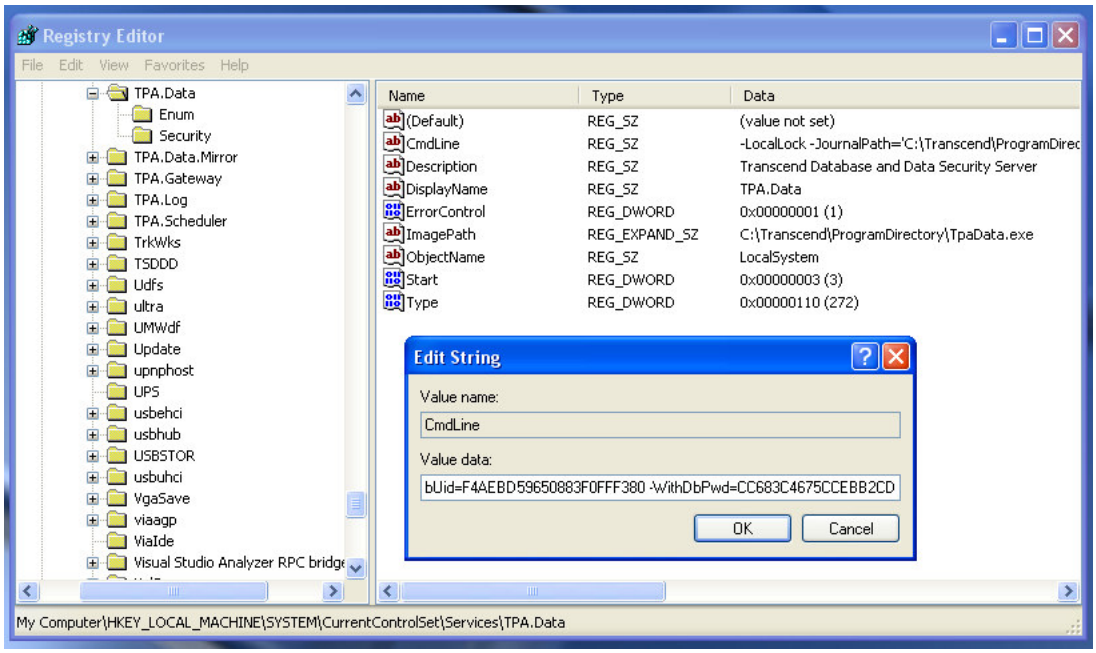


Figure Four

E N D O F D O C U M E N T

T H I S P A G E I S L E F T I N T E N T I O N A L L Y B L A N K